Université de Gafsa

Institut Supérieur des Sciences Appliquées et de Technologie de GAFSA

Département de Informatique et télécommunication

Réalisation d'un système de détection des intrusions basé sur RaspBerry

Malek issaoui & jihen Allegui

En vue de l'obtention de

Sous la Direction de :

Mr.Telli Mounir

Mr. Ilyes Soualmia (CPG)

Soutenu le 05/06/20223

Devant le jury composé de :

Président :

Rapporteur :

Membres :

2022/2023

Dédicaces

Tout d'abord merci à mon DIEU de m'avoir donné la force pour terminer ce travail.
Je dédie ce travail à tous ceux qui m'ont aidé à réaliser ce travail.

❖ *A ma mère*
J'espère qu'elle le trouve récompensant de tous les sacrifices qu'elle consenti pour moi

❖ *A mes sœurs*

Malek Issaoui

Dédicaces

Tout d'abord merci à mon DIEU de m'avoir donné la force pour terminer ce travail.
Je dédie ce travail à tous ceux qui m'ont aidé à réaliser ce travail.

❖ *A ma mère*
J'espère qu'elle le trouve récompensant de tous les sacrifices qu'elle consenti pour moi

❖ *A mes sœurs*

Jihen Allegui

Remerciements

Je tiens a présenter mes reconnaissances et mes remerciements a mon professeur encadrant ***M.Telli mounir*** pour le temps consacré a la lecture et aux réunions qui ont rythmées les différentes étapes de mon projet de fin d'étude .Je remercie aussi pour leur disponibilité a encadrer ce travail a travers leur critique et leur proposition d'amélioration.

Sommaire

Liste des figures

Liste des Tableaux

Introduction Générale

La sécurité est devenue une préoccupation majeure de la plupart des gens, d'autant plus que la plupart des pays développés ont enregistré une hausse significative des cambriolages de maison et des entreprises dans les dernières décennies. Renforcer la sécurité d'une maison ou siège d'établissement est la première étape dans la prévention des cambriolages .En premier lieu, il s'agit d'évaluer l'accessibilité d'un cambrioleur dans le domicile. Il est nécessaire de tout mettre en œuvre en mettant un bon système de sécurité pour diminuer le risque d'intrusion dans une habitation.

Un système d'alarme moderne et professionnel doit comporter impérativement des détecteurs qui pourraient détecter tout événement pouvant mettre en danger les biens ou la vie humaine telle que les incendies, l'agression, le cambriolage, le vandalisme ...etc. également un système d'alarme doit comporter une centrale d'alarme programmable et des avertisseurs pour signaler la production d'un événement.

Dans ce travail, nous proposons la réalisation d'un système d'alarme fonctionnant identiquement que les systèmes d'alarme commercialisées actuellement. Notre système est constitué à base d'une carte Arduino Pro Mini et il est programmable selon le besoin et le lieu à surveiller.

Pour ce projet de fin d'étude nous nous proposons d'étudier la système de détection des intrusions. Pour ce faire nous avons organisé notre travail en trois chapitres.

- Dans le premier chapitre, nous présentons le contexte de notre projet et les problématiques les plus répandues, nous décrivons le fonctionnement et le principe de notresolution proposée.
- Le Deuxième chapitre, nous concerne aussi bien les besoins pour réalisés notre Système (software, hardware).
- Le troisième chapitre nous avons détaillé notre système réalisé.

Chapitre 1 : Etat de l’art

1. Introduction

Surveillance d'entrepôts, d'entreprises, d'usines, de magasins, de bureaux…, les lieux nécessitant la présence des professionnels de la sécurité sont multiples.

Afin d'assurer cette mission, les entreprises font de plus en plus appel à des sociétés extérieures. Le nombre de personnes embauchées pour cela ne cesse d'augmenter dans le monde entier. L'installation des systèmes de détection doit être réalisée avec une grande précision par des professionnels spécialisés et dûment qualifiés

Une administration, une entreprise publique ou privée doit assurer la sécurité des personnes et des biens, à la prévention et à la lutte contre les sinistres et les risques professionnels : incendie, bris de machine, vols, intrusion … etc.

Dans ce chapitre, nous décrivons le contexte général du projet. Nous présentons d'abord les problèmes et la solution proposée et nous enchainons par la suite par l'exposé du sujet en expliquant ses la technologie utilisée.

2. Cadre de projet

Dans cette partie nous présentons l'organisme dans lequel nous avons effectué notre stage de projet de fin d'étude.

2.1. Présentation de la société

CPG est une entreprise tunisienne d'exploitation des phosphates basée à Gafsa. La CPG figure parmi les plus importants producteurs de phosphates, occupant la cinquième place mondiale. L'activité de l'entreprise se définit en 4 grands groupes : La préparation du terrain, extraction, production et la commercialisation des phosphates.

2.2. Historique de la société

C'était en avril 1985, lors d'une prospection dans la région de Métlaoui, partie occidentale du sud du pays, que Philippe THOMAS, géologue amateur français, a découvert des couches puissantes de phosphates de calcium sur le versant nord de Jebel THELJA. D'autres prospections géologiques et des explorations de grande envergure ont suivi cette découverte décisive. Celles-ci ont révélé l'existence d'important gisement de phosphates au sud et au nord de l'île de Kasserine.

A partir de 1896 date de création de la « compagnie des phosphates de chemin de fer de Gafsa », une nouvelle activité industrielle des phosphates a vu le jour dans le pays. Les premières excavations ont commencé dans la région de Métlaoui et vers 1900, la production de

phosphate marchand a atteint un niveau de 200.000 tonnes. Après ces débuts, la Compagnie des phosphates et de chemin de fer de Gafsa a connu tout au long de sa longue histoire une série de changements structurels avant d'acquérir son statut actuel et de devenir en janvier 1976, la compagnie des phosphates de Gafsa – CPG – Avec une expérience centenaire dans l'exploitation et la commercialisation des phosphates tunisiens, la CPG figure parmi les plus gros producteurs de phosphate dans le monde. Elle occupe le 5ème rang à l'échelle mondial avec une production actuelle excédant 8 millions de tonnes de phosphates marchand.

2.3. Organigramme de la CPG

Le diagramme suivant explicite la répartition des différents organes de la CPG :

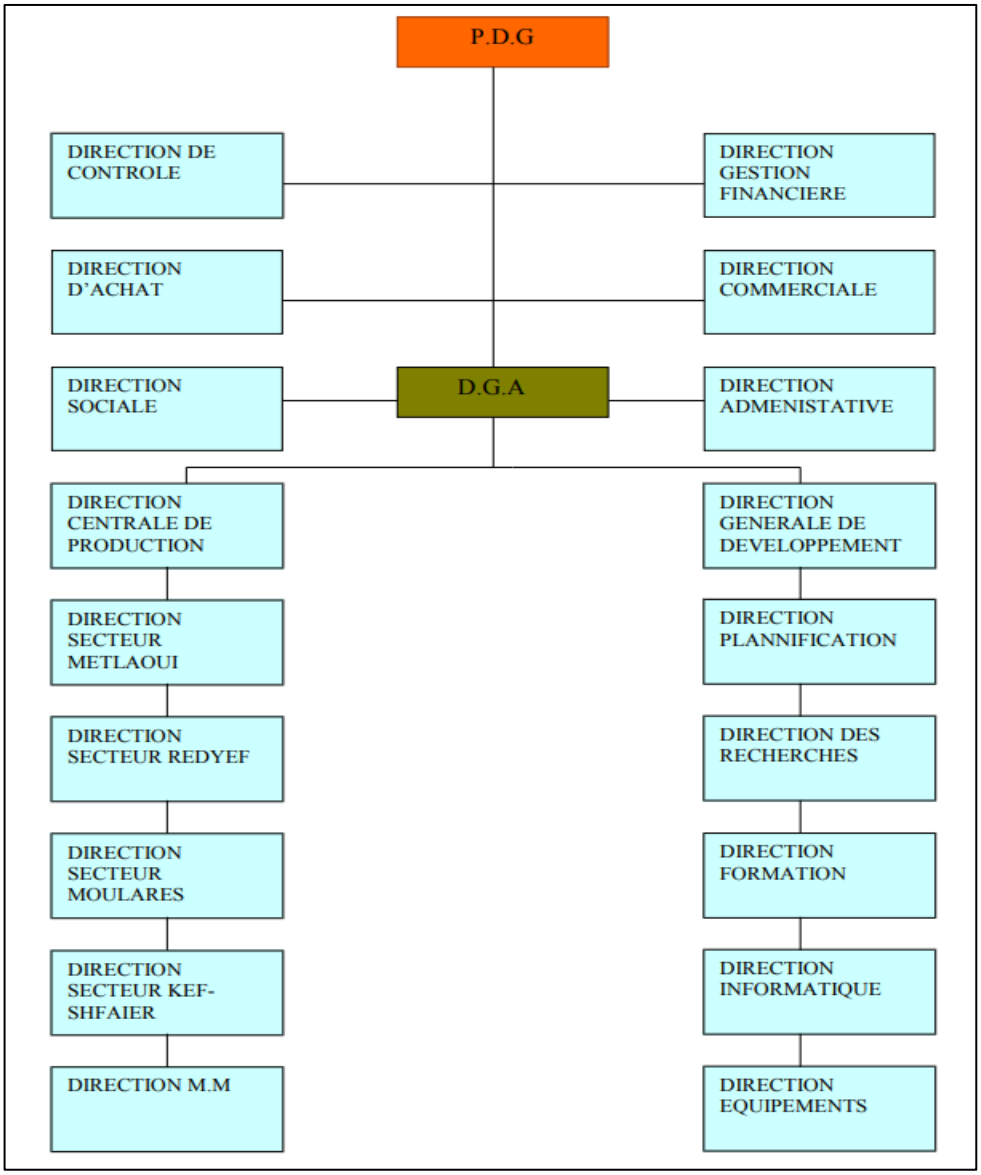

FIGURE 1-0-1 : ORGANIGRAMME DE LA CPG

3. Contexte du Projet

L'évolution de la technologie et du mode de vie nous permet aujourd'hui de prévoir des espaces de travail et de logement mieux adaptés, tant en nouvelle construction qu'en rénovation. Nous devons ces nouvelles possibilités principalement aux progrès réalisés en électronique et à la nouvelle conception des réseaux de communication tant à l'intérieur qu'à l'extérieur des entreprises.

La technologie ouvre non seulement de nouvelles possibilités dans le domaine de sécurité, mais constitue aussi et surtout un moyen offert à l'individu de sécurisé son environnement. Grâce à cette nouvelle technologie, l'habitant sera à même de mieux gérer son milieu de travail et de vie sur le plan de la sécurité, du confort, des communications.

4. Problématique

Avec la croissance des technologies, les entreprises sont dorénavant les lieux les plus importants dans une entreprise.

Les données stockées dans une entreprise sont donc d'une grande valeur et doivent être dans un emplacement sécurisé, sécuritaire et protégé.

Quand on parle de problème des environnements dans les entreprises, il ne faut pas oublier la fondation, qui est la problème physique' des équipements critiques, tels que serveurs, équipements de télécommunications, routeur/pare-feu, etc.

Contrôlerles déplacements et le vas et vient des utilisateurs dans la salle pour contrôler le temps de travail d'un part; d'autre part pour sécuriser l'entreprise contre les interventionsextérieur.

4.1. Solution proposée

Notre projet « **système de détection des intrusions**» a été proposé dans le but de répondre à un ensemble de besoin qui spécifient précisément les services demandés et attendus par La CPG. Ces services, qui sont regroupés sous les termes « sécurité» et « automatiques » coincement principalement la sécurisé. En effet, notre solution consiste à faire l'implementation d'un système de detection d'intrusion à base de RaspBerry.

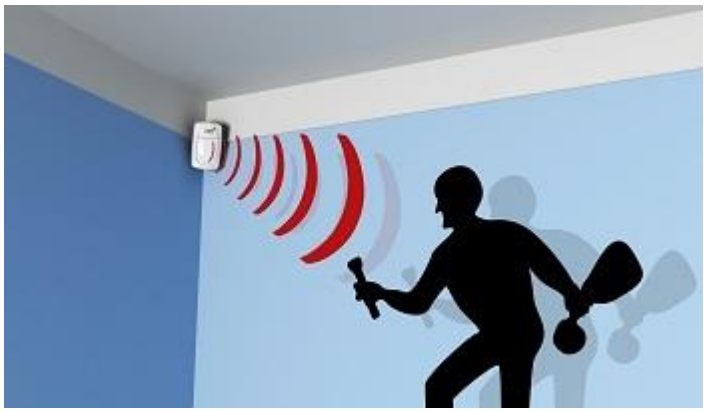

FIGURE 1. 1: SYSTEME DE DETECTION DES INTRUSIONS

Notre projet a pour objectifs de :

- La détection d'une présence ou d'une intrusion (détecteur de mouvement ou d'accès)
- La gestion automatique de la sonnerie d'alarme en cas de détection des intrusions
- La gestion automatique d'alarme.
- Éviter les problèmes liés à la vérification de l'entreprise et de ses équipements.

4.2. L'objectif technique

Pour que l'espace fonctionne comme on le souhaite, nous avons mis en place un certain nombre de capteurs, d'effecteurs et de modules de communication qui vont être orchestrés par un module Arduino. Ces composants sont détaillés dans ce qui suit.

Nous avons fixé notre cahier des charges du projet dont les points suivants seront recouverts :

- Nous devons d'abord concevoir l'espace dans lequel le système fonctionnera par exemple entreprise
- Établir les fonctions de la domotique suivantes :
  - Un détecteur de mouvement

Afin de concrétiser notre projet, nous allons passer par les étapes suivantes :

- Etude générale du système domotique.
- Etude du fonctionnement de chaque partie du système.
- Réalisation et conception du projet (Réalisation du prototype).
- Test de fonctionnement du prototype de notre projet.

5. Généralité sur la sécurité

5.1. Définition de la sécurité

La sécurité désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux risques techniques, physiques, chimiques et environnementaux pouvant nuire aux personnes et aux biens sans avoir un but de profit.

Un système de sécurité est un système électronique destiné à prévenir et empêcher la présence d'un corps étranger, fixés aux produits à protéger et des portiques de détection situés aux différents points, Lorsqu'un corps pénètre dans le champ de détection des portiques, une alarme visuelle et/ou sonore se déclenche, alertant le personnel.

La sécurité se dit d'une situation où l'on n'a aucun danger à craindre. Cette définition générale, reposant sur le principe du risque zéro, n'est pas adaptée aux activités humaines (alimentation, transport, vie quotidienne, loisirs, etc.) où l'on parle de risque acceptable. Se référant à l'industrie et, plus particulièrement, au fonctionnement des procédés, la sécurité peut être définie comme l'aptitude d'un système à fonctionner en maîtrisant, à un niveau acceptable, les risques pour les personnes, les biens et l'environnement.

5.1.1. Sécurité physique

La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, Dans la sécurité physique, on peut intégrer :

- la gestion et sécurisation des flux de biens et de personnes
- la surveillance de son entreprise.
- la protection périmétrique de son entreprise.
- la prévention des malveillances

FIGURE 1. 2: LA SECURITE PHYSIQUE

5.1.2. Sécurité logique

La sécurité logique est la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation. Dans la sécurité logique, on peut intégrer :

- la gestion et la sécurisation des accès informatiques et des identités
- la protection des données et des systèmes d'informations
- la sécurisation des réseaux et des infrastructures informatiques et de technologiques
- la sécurité liée aux nouvelles technologies (applications...)

5.2. L'importance de la sécurité

Sécurité bancaire, sécurité alimentaire, sécurité informatique, sécurité routière, sécurité sociale et bien d'autres, la sécurité implique un règlement à suivre, des normes à respecter pour tous. La sécurité, c'est aussi un moyen qui nous permet de vivre en communauté ; il existe des règles plus ou moins contraignantes qui visent à faire cohabiter les humains entre eux. La sécurité est donc pour nous un élément incontournable de notre quotidien. [1]

6. Présentation de l'Internet des Objets

6.1. Définition

Il y a plusieurs définition du concept Internet des Objets (en anglais : Internet of Things ou IoT). Dans ce qui suit, on présente quelques définitions.

- **Premier Définition**

Internet des Objets est un réseau qui relie et combine les objets avec l'Internet suivant des protocoles qui assurent leur communication et échange d'informations à travers une variété de dispositifs [2].

- **Deuxième Définition**

L'Internet des objets peut être défini aussi comme étant un réseau de réseaux qui permet, via des systèmes d'identification électroniques normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi, de pouvoir récupérer, stocker, transférer et traiter les données sans discontinuité entre les mondes physiques et virtuels.

6.2. Historique sur l'Internet des objets

Le terme « Internet of Things » (en Français Internet des Objets) est né en 1999 au centre MIT (Massachusetts Institute of Technology), grâce à Kevin Ashton, un chercheur britannique, pionnier dans son domaine (IDO). Son équipe a lancer la promotion d'une connectivité ouverte de tous les objets en utilisant les étiquettes RFID (Radio Frequency Identification). Grâce à l'apparition du nouveau protocole IPv6, des secteurs comme l'aéronautique s'emparent rapidement du concept de l'Internet des objets, et participent aux recherches. Ce concept de l'Internet des Objets commence à connaitre une popularité en 2007. Nous avons envisagé alors de mettre en place un Internet des Objets Global, Ubiquitaire.

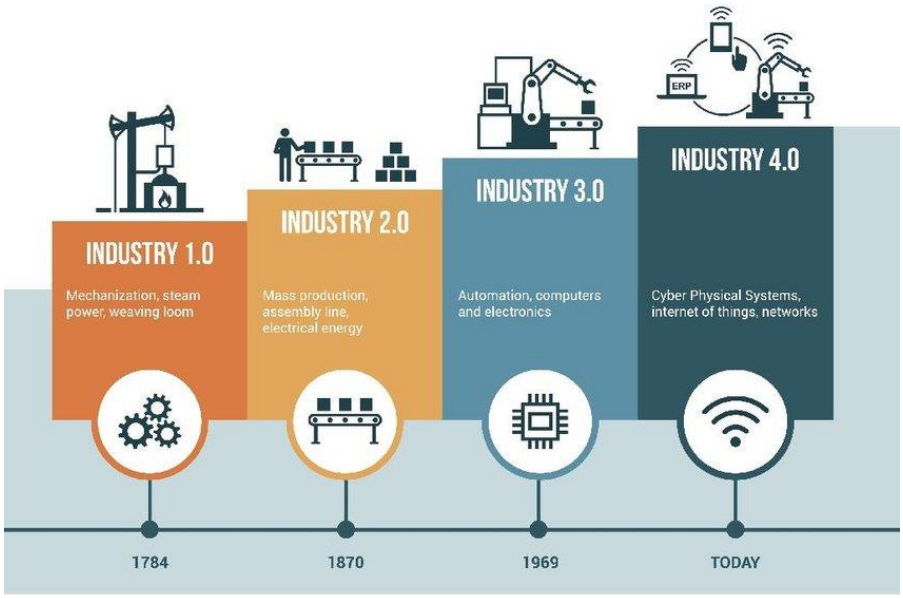

FIGURE 1. 3: HISTORIQUE SUR L'INTERNET DES OBJETS[3]

6.3. Concept d'IOT

L'IoT est l'interconnexion de toutes les machines, des objets vivants et des éléments non-vivants intégrés aux capteurs, aux actionneurs, à l'électronique, aux logiciels et à la connectivité réseau avec la possibilité de transférer des données sur un réseau sans la nécessité de la participation de l'homme ou l'interaction homme-ordinateur. L'IoT permet aux objets d'être détectés ou contrôlés à distance à travers l'infrastructure du réseau existante, créant des opportunités pour une intégration plus directe du monde physique dans les systèmes informatiques entraînant une efficacité, une précision et des avantages économiques améliorés en plus d'une intervention humaine réduite.

Pour notre projet, nous devons acquérir une connaissance de l'architecture de l'IoT. Il y a quatre couches d'architecture IoT : la couche interface, la couche de traitement, la couche réseau, la couche service et la couche de détection.

- **Couche d'interface**

C'est la première couche de l'architecture IoT. Cette couche fournit les méthodes d'interaction entre les utilisateurs et l'application. Pour cela, nous devons créer une page Web ou une application mobile qui interagit avec les périphériques avec la couche de traitement des événements.

- **Couche de service**

Cette couche est utilisée pour créer et gérer des services répondant aux besoins de l'utilisateur. Pour ce faire, elle traite le traitement en profondeur des données. Pour rendre l'application plus conviviale, elle fournit une base de données et divise le travail. C'est une couche importante pour trois raisons :

- La possibilité de prendre en charge un serveur HTTP et / ou un courtier MQTT pour communiquer avec les périphériques.
- La possibilité d'agréger et de combiner les communications de différents dispositifs de détection et d'acheminer les communications vers un dispositif spécifique (éventuellement via un blindage Ethernet / GSM / GPRS).
- Possibilité de passerelle et de se transformer entre différents protocoles afin de proposer des API HTTP basées sur un message MQTT envoyé au périphérique.

❖ **Couche réseau**

Internet, réseau de communication mobile, réseau de communication par satellite, réseau de télévision par câble, centre d'information, centre de gestion de réseau.

❖ **Couche de détection**

Lecteur RFID, réseau de capteurs, réseau d'accès, étiquette RFID, capteurs, terminal intelligent etc.

6.4. Architecture d'un système IdO

En fait, il n'y a pas une définition formellement identique d'une architecture d'un système IdO adoptée par tous les projets(10). Dans le ce mémoire on adopte celle présentée dans illustrée par la Tableau 5 Cette architecture est composée de trois couches :

TABLEAU 1. 1: ARCHITECTURE DE L'IDO [4]

Couche Application	Application IdO
	Support d'application
Couche transmission	Réseau local étendu
	Réseau cœur
	Réseau d'accès
Couche perception	Réseau de perception
	Nœud de perception

➢ **Couche de Perception**

La couche de perception (peut être appelé "couche de périphérique", "couche sensorielle" ou "couche de reconnaissance") qui est la couche la plus basse de l'architecture IoT,

est responsable de la capture des informations du monde réel et leur représentation au format numérique. Elle inclut les technologies utilisées pour la détection (collecte des données de l'environnement), l'identification (identification d'objets), l'activation (réalisation données détectées) et la communication (établissement de la connectivité entre appareils intelligents hétérogènes) avec un minimum d'interaction humaine. Selon les fonctionnalités qu'elle assure, cette couche peut être divisée en deux sous-couches: les nœuds de perception (ou nœuds sensoriels) et le réseau de perception (comme réseau des capteurs).

- **Couche de Transmission**

La couche de transmission (appelée aussi «couche de transport» ou «couche réseau») est responsable de transmission des données collectées par les nœuds de perception à l'unité de traitement de l'information (ou unités de prise de décision de haut niveau) à travers un réseau ou une interconnexion des réseaux. Cette couche permet alors une intégration d'une variété de réseaux, de technologies et de protocoles hétérogènes.

Cette couche peut être divisée en trois sous-couches: réseau d'accès, réseau cœur et réseau local et étendu.

- **Couche Application**

C'est la couche la plus haute de l'architecture IoT visible par l'utilisateur final. La couche application a pour but de gérer et de fournir les applications globales en se basant sur la les informations collectées par la couche de perception. Elle fournit aux utilisateurs finaux un accès aux services personnalisés sur le réseau, en fonction de leurs besoins, grâce à l'utilisation de divers appareils mobiles et équipements terminaux.

Cette couche peut être divisée en deux sous-couches: couche de support d'application et applications IdO.

6.5. Domaines d'application de l'IdO

Les applications potentielles de l'IdO sont nombreuses et variées, pénétrant dans pratiquement tous les domaines de la vie quotidienne des individus, des entreprises et de la société dans son ensemble.

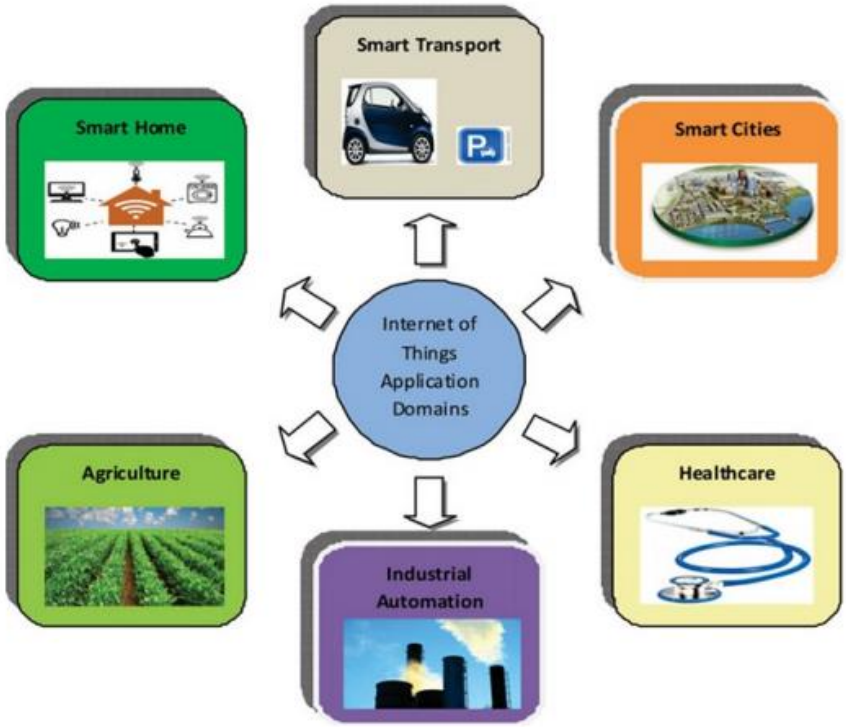

FIGURE 1. 4: DOMAINE IOT [4]

En fonction de leurs fonctionnalités, les applications IdO peuvent être divisées en trois catégories :

- applications de collection d'informations : elles sont chargées de collecter les données des nœuds de perception et de leur stockage local
- applications d'analyse : elles sont concernées par le prétraitement hors ligne des données collectées pour créer un modèle générique à utiliser pour l'évaluation de futures données à collecter ultérieurement
- applications prise de décision en temps réel : elles sont impliquées dans la prise des mesures et actions appropriées en fonction des données capturées et analysées.

6.6. L'architecture de l'Internet des objets

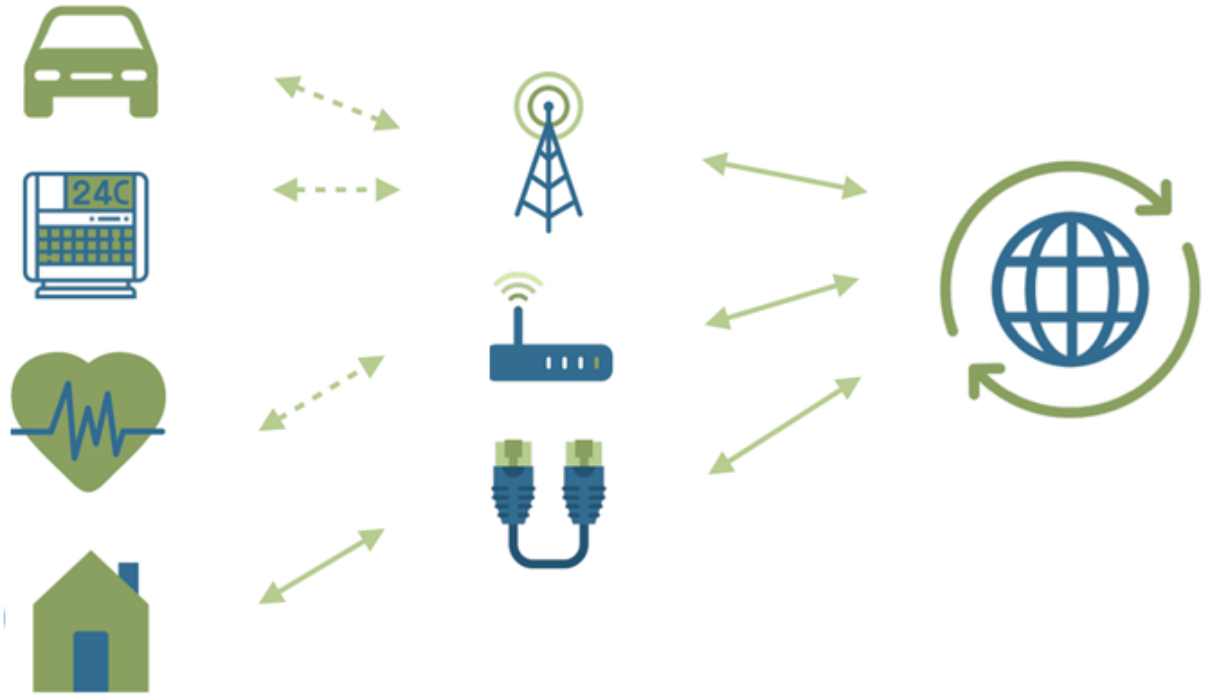

FIGURE 1. 5: L'ARCHITECTURE DE L'INTERNET DES OBJETS

Précisons le rôle des différents processus présentés sur ce schéma :

- ✓ Capter désigne l'action de transformer une grandeur physique analogique en un signal numérique.
- ✓ Concentrer permet d'interfacer un réseau spécialisé d'objet à un réseau IP standard ou des dispositifs grand public.
- ✓ Stocker qualifie le fait d'agréger des données brutes, produites en temps réel, méta taguées, arrivant de façon non prédictible.
- ✓ Enfin, présenter indique la capacité de restituer les informations de façon compréhensible par l'Homme, tout en lui offrant un moyen d'agir et/ou d'interagir.

Deux autres processus n'apparaissent pas sur le schéma, car ils sont à la fois transverses et omniprésents :

- ✓ Le traitement des données est un processus qui peut intervenir à tous les niveaux de la chaîne, depuis la capture de l'information jusqu'à sa restitution. Une stratégie pertinente, et commune quand on parle d'Internet des objets, consiste à stocker l'information dans sa forme intégrale. On collecte de manière exhaustive, « big data », sans préjuger des traitements qu'on fera subir aux

données. Cette stratégie est possible aujourd'hui grâce à des architectures distribuées type NoSQL, capables d'emmagasiner de grandes quantités d'information tout en offrant la possibilité de réaliser des traitements complexes en leur sein (Map/Reduce par exemple).

La transmission des données est un processus qui intervient à tous les niveaux de la Chaîne. Deux réseaux, supports des transmissions, cohabitent généralement :

- ✓ Réseau local de concentration. On utilise alors des technologies comme ANT, Zig Bee, Z-Waves, NFC ou Bluetooth LE.
- ✓ Réseau WAN, permettant d'interconnecter les réseaux spécialisés et de les interfacer avec des fermes de serveur. On utilise alors Wifi, les réseaux cellulaires (GSM, UMTS, LTE) ou encore les connexions physiques standard (Ethernet, fibre optique). Ces réseaux sont généralement connectés à Internet [5].

7. Conclusion

Dans ce chapitre, nous avons essayé d'expliquer le contexte du projet et dévoiler l'objectif du travail demandé. En fin nous avons présenté une vue générale sur les système d'alarme.

Dans les chapitres qui vont suivre, nous allons détailler petit à petit la conception, la réalisation et l'intégration des différents composants de notre système.

Chapitre 2 : Etude de la partie matérielle et logiciels du projet

1. Introduction

Dans ce chapitre, nous allons discuter l'automatisation du prototype de ce projet que nous proposons. En première partie, il sera introduit par les équipements qui donnera une vision générale sur les composants électroniques à utiliser. Ensuite, une deuxième partie qui traitera la programmation.

2. Etude de la partie matérielle

Dans le cadre de ce travail, nous adapterons un modèle qui permet la supervision à distance d'un réseau tout en assurant la disponibilité permanente de l'information pour aider à prendre des décisions en temps réel selon un état présent. Pour ce faire nous allons détailler en ce qui suit les choix du matériel intelligent et du logiciel adoptés dans notre approche.

Nous allons aborder cette partie par les différents organes utilisés dans notre système :

2.1. Choix de la carte programmable

Les cibles embarquées présentes ci-dessous nous ont permis d'implémenter notre système et de respecter les différents critères tels que la communication à distance via un réseau internet et l'espace mémoire pour stocker les informations envoyées par les capteurs intelligents :

2.1.1. La Carte raspberry pi

Le Raspberry Pi est un nano-ordinateur monocarte à processeur ARM de la taille d'une carte de crédit conçu par des professeurs du département informatique de l'université de Cambridge dans le cadre de la fondation Raspberry Pi. Le Raspberry Pi fut créé afin de démocratiser l'accès aux ordinateurs et au digital making.

- **Comparaison de différents types de modèles Raspberry Pi**

Le Raspberry Pi est une série de petits ordinateurs monocartes développés au Royaume-Uni par la Fondation Raspberry Pi pour promouvoir l'enseignement de l'informatique de base dans les écoles et dans les pays en développement. Le modèle original est devenu beaucoup plus populaire que prévu, se vendant en dehors de son marché cible pour des utilisations telles

que la robotique. Les comparaisons entre les Raspberry Pi vendus sur le marché actuellement sont données ci-dessous.

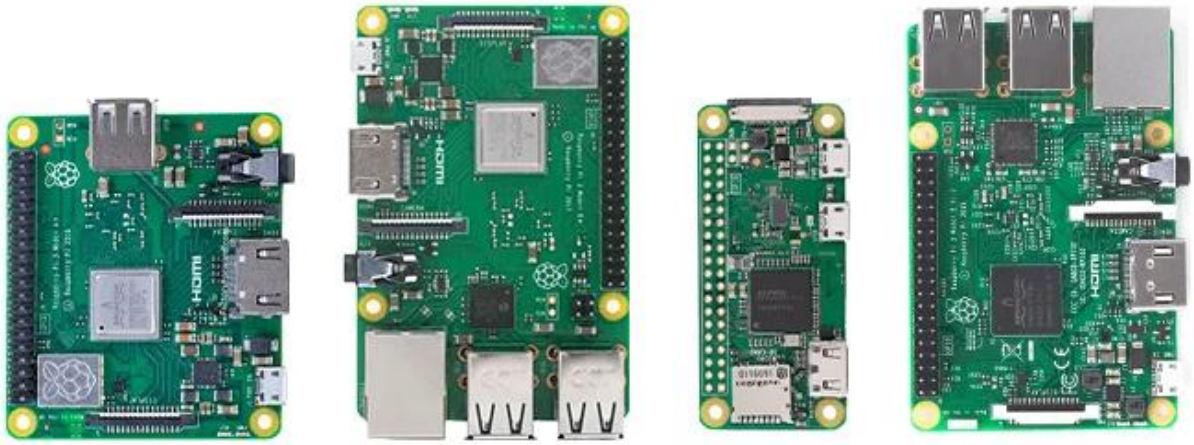

FIGURE 2. 1: LES DIFFERENTES CARTES RASPBERRY. [7]

2.1.2. Choix de la carte proposé (Module Raspberry Pi)

Plusieurs types de systèmes embarqués existent. Les systèmes fortement contraints nécessitant une grande puissance de calcul requièrent des cycles de développement lourds et coûteux. Les électroniques mettent en œuvre des technologies onéreuses et en faibles quantités. Les évolutions technologiques ont permis :

- D'avoir des processeurs de plus en plus puissants, consommant de moins en moins, des coûts de plus en plus réduits.
- La venue du logiciel libre (avec ses avantages et ses inconvénients) a permis une démocratisation du développement logiciel.

On doit trouver un système qui regroupe un bon nombre d'éléments habituellement disponibles que sur des plateformes lourdes (puissance de calcul, périphériques entrée/sortie, environnement logiciel libre) sur un format facilement embarquant, à un prix défiant toute concurrence et facile a programmé à savoir le Raspberry PI3

FIGURE 2. 2: RASPBERRY PI 2 MODEL B

Les premiers prototypes du Raspberry Pi sont développés sur des microcontrôleurs Atmel ATmega 644. Ce Microordinateur s'inspire du BBC Micro d'Acorn Computer (1981) et est destiné à encourager la jeunesse à la programmation. Le model B a été lancé en février 2015 Avec 900MHz Quad-Core ARM-cotre-A7 CPU

- 1GB de RAM
- 4 ports USB
- Full HDMI port
- Port Ethernet
- Prise jack 3.5mm
- Interface d'une smart camera
- Interface d'un écran
- Lecteur de carte mémoire
- VidéoCore IV 3D graphique

Il s'agit tout simplement un microordinateur qui a des caractéristiques d'un smartphone de milieu de gamme et critiquable au niveau de :

- utilisation carte SD pas suffisamment fiable.
- tenue en température.

Toutefois elle offre des avantages non négligeables :

- puissance de calcul importante
- interfaçage facile : UART, USB, Ethernet, Picamera

- Faible coût

2.1.3. Spécification du Raspberry

Le Raspberry Pi est une série de nano-ordinateurs mono-carte (avec un processeur ARM) développé en Angleterre par David Braben (un créateur de jeux-vidéos) dans le cadre de la fondation « Raspberry Pi Foundation » afin de promouvoir l'apprentissage des sciences de l'informatique dans les écoles des pays en voie de développement. Cet ordinateur ayant la taille d'une carte de crédit permet l'utilisation de nombreux systèmes d'exploitation, en particulier GNU/Linux. Le premier modèle s'est répandu plus vite que ce qui était prévu avec des utilisations comme la robotique. Les périphériques comme les claviers, souris et boitiers ne sont pas inclus avec le Raspberry Pi dans l'optique de réduire les coûts et réutiliser du matériel mais des accessoires ont été inclus dans des packs officiels ou non.

Du coté hardware, la plupart des modèles suivent la représentation suivante, à l'exception des modèles A, A+ et Zero qui ne possèdent pas de connexion Ethernet et de ports USB.

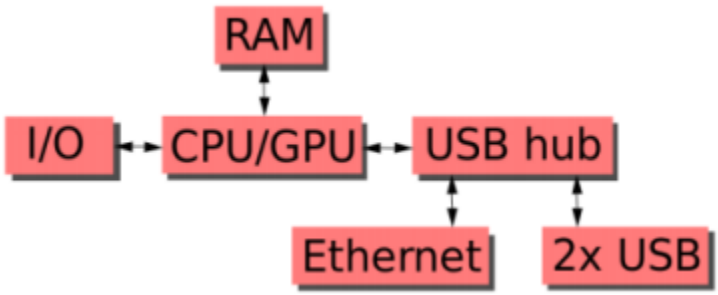

FIGURE 2. 3: DIAGRAMME REPRESENTANT LES INTERACTIONS ENTRE LES COMPOSANTS DU RASPBERRY

Le Raspberry PI2 contient certaines nouveautés par rapport à ses prédécesseurs. Nous pouvons sur la figure suivante les différentes constitutions d'un raspberry PI2.

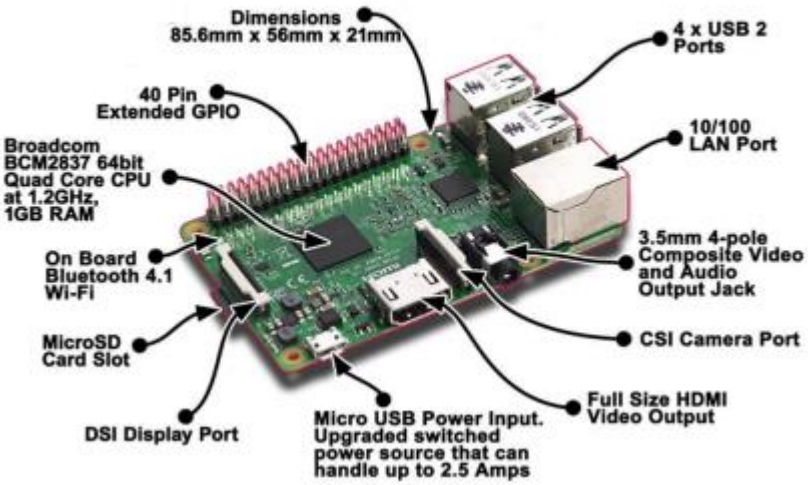

FIGURE 2. 4: CERTAINES DES NOUVEAUTES INCLUSES DANS LE RASPBERRY PI 2

2.2. Les Accessoires de la carte Raspberry

2.2.1. Les modules

❖ **Module sonore « Buzzer » :**

Les buzzers peuvent être trouvés dans les dispositifs d'alarme, les ordinateurs, les minuteries et la confirmation de l'entrée utilisateur, il s'agit d'une tonalité continue avec une sortie sonore minimale de 70 dB à 1 m pour sa taille. Il est doté d'une puissance électrique nominale de 3 V et 150 mA.[8]

FIGURE 2. 5: UN PIEZO-ELECTRIQUE (BUZZER).

TABLEAU 2. 1: DESCRIPTION ET AVANTAGE DE BUZZER

Description	• Type : Buzzer passive • Tension de travail : 3.5-5.5v • Courant de travail : < 25mA

	• Dimension PCB : 18.5mm x 15mm (L x P) • Fonction de Buzzer : buzz
Avantages de Buzzer	✍ Bon marché, ✍ Contrôle de la fréquence sonore, vous pouvez faire un "plus que l'efficacité d'un cheveu mètre Suola Xi 'Fruit. ✍ Dans certains cas particuliers, vous pouvez réutiliser un contrôle et un port LED Buzzer actif ✍ Contrôle de processus ✍ Pratique.

➢ **Caractéristiques techniques du buzzer : [8]**

- Dimensions : diamètre approximatif de 12 mm, hauteur 9mm.
- Type de sonnerie : continue.
- Tension d'alimentation : 2V - 4V.
- Couleur du corps : noir.
- 2 broches : positive et négative.

❖ **Module Ethernet**

➢ **La carte Ethernet Shield**

L'Ethernet Shield (figure 2.4) permet de relier la carte de contrôle décrite dans le paragraphe précèdent (Arduino UNO) à l'internet. Cette carte donne l'accès au réseau à travers un câble RG45. Il est basé sur le microprocesseur Wiznet W5100 (figure 2.5).[9]La carte Ethernet Shield nécessite les éléments suivants :

➢ Carte de contrôle Arduino UNO.

- Câble RG45.
- SD Card (carte mémoire).
- Routeur qui donne l'accès à l'internet (vitesse de la connexion 10/100Mb)

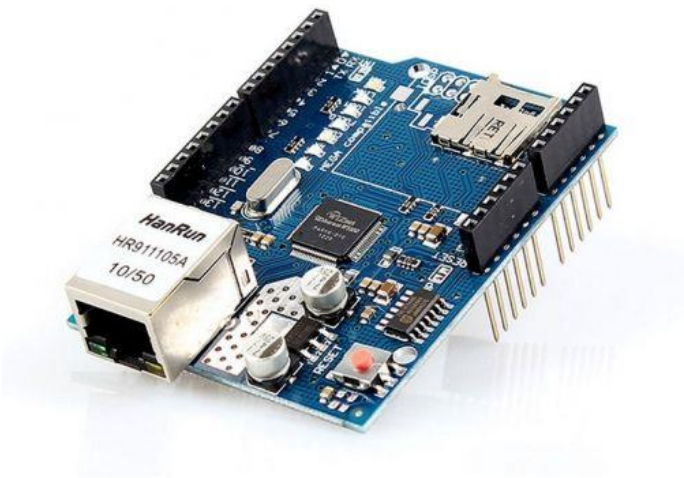

FIGURE 2. 6: LA CARTE ETHERNET SHIELD [9]

FIGURE 2. 7: LE MICROPROCESSEUR W5100

✓ **Les caractéristiques de l'Ethernet Shield**

La carte Ethernet Shield dispose les caractéristiques suivantes (voir figure 2.6) :

- Interface d'entrée pour la carte mémoire pour stocker les données.
- Interface pour le câble RG45.
- Connecter à l'Arduino à travers l'interface SPI (Serial Perepheral Interface)
- Taille : 55.88mm X 68.58mm X 1.6mm.

- Alimentation : 5V.
- Des indicateurs LED : TX, RX, COL, FEX, SPD, LNK.
    - LED TX : Clignote quand la carte envoie les données.
    - LED RX : Clignote quand la carte reçoit les données.
    - LED COL : Clignote quand il y la collision dans le réseau.
    - LED FEX : Indique que la connexion est dans le mode Full-duplex.
    - LED SPD : Indique que la vitesse de la connexion est 100Mb/s.
    - LED LNK : Indique la présence d'une liaison réseau et clignoté quand la carte transmit ou reçoit les données.

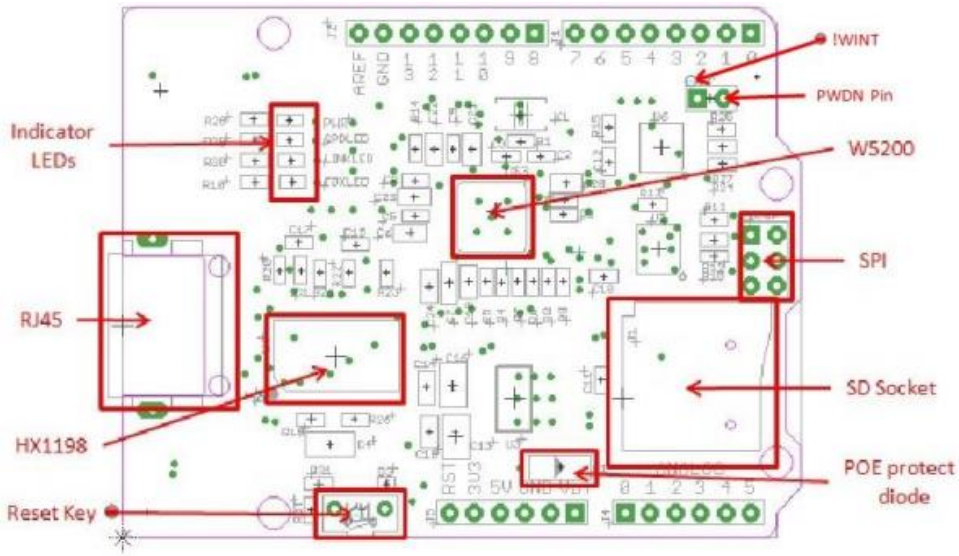

FIGURE 2. 8: INTERFACE HARDWARE DE LA CARTE ETHERNET SHIELD

3. Installation/configuration du deux Raspberries

3.1. Choix de la distribution

Le Raspberry Pi peut fonctionner sous de nombreux systèmes d'exploitation qui sont compatibles avec l'architecture ARM :

- Debian : qui a une version dédiée appelée Raspbian (avant avec le kernel Wheezy et puis maintenant avec Jessie), ce système est recommandé par la fondation Raspberry PI
- Ubuntu Mate et Snappy Ubuntu : basé sur Ubuntu, Snappy Ubuntu est plus réservé aux développeurs.
- Fedora : un autre système d'exploitation libre et une distribution GNU/Linux. Arch Linux : encore une distribution Linux qui met en avant la simplicité.

- Gentoo Linux, Slackware et Suse qui sont des distributions Linux.
- RISC OS : un système d'exploitation spécialement conçu pour les architecture ARM.
- NetBSD : un système d'exploitation libre de type Unix BSD.
- Kali Linux : anciennement Backtrack, ce système d'exploitation possède tous les outils nécessaires aux tests de sécurité d'un système d'information.
- Windows 10 IOT : Windows 10 spécialement conçu pour les objets connectés.
- OSMC : Media center gratuit et libre, basé sur du Linux.
- LibreElec : évolution de OpenElec, un autre media center.

Au démarrage du Raspberry Pi avec une carte MicroSD ayant NOOBS chargé dessus, c'est le menu que l'on obtient (figure ci-dessous).

FIGURE 2. 9: MENU DE DEMARRAGE DU RASPBERRY PI AVEC UNE CARTE MICROSD AVEC NOOBS

A titre de comparaisons entre les systèmes d'exploitation Raspbian et Debian il faut savoir que Raspbian est un portage non officiel de Debian Wheezy ARMhf (Arm Hard Float Port). Les architectures ARM, sont des architectures matérielles RISC (Reduced Instruction set computer, traduit littéralement par processeur à jeu d'instructions réduit). On ne peut donc pas installer les paquets de la même manière sur une architecture ARMhf et AMD64/i386 (Debian). Il va donc falloir utiliser ce qu'on appelle de la compilation croisée.

Une chaîne de compilation croisée est une chaîne compilée pour fonctionner sur l'architecture de processeurs de la machine hôte, mais qui va compiler des logiciels pour une architecture cible différente. La compilation croisée fait donc référence aux chaînes de compilation capables de traduire un code source en code objet dont l'architecture processeur diffère de celle où la compilation est effectuée. Ces chaînes sont principalement utilisées en informatique industrielle et dans les systèmes embarqués.

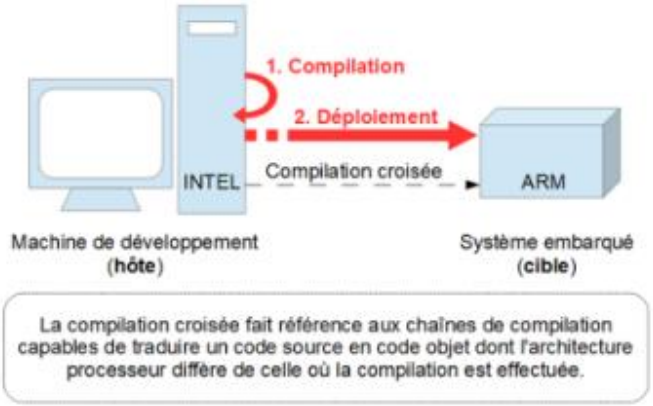

FIGURE 2. 10:SCHEMA DU FONCTIONNEMENT DE LA COMPILATION CROISEE.

4. Installation et configuration de Raspbian

Il faut commencer par préparer la carte SD depuis Windows afin que celle-ci intègre Raspbian et non NOOBS. On peut utiliser le logiciel Win32DiskImager pour ce faire. Les performances du Raspberry Pi sont fortement influencées par la qualité de la carte SD on a donc choisi une carte SD de 32Go.

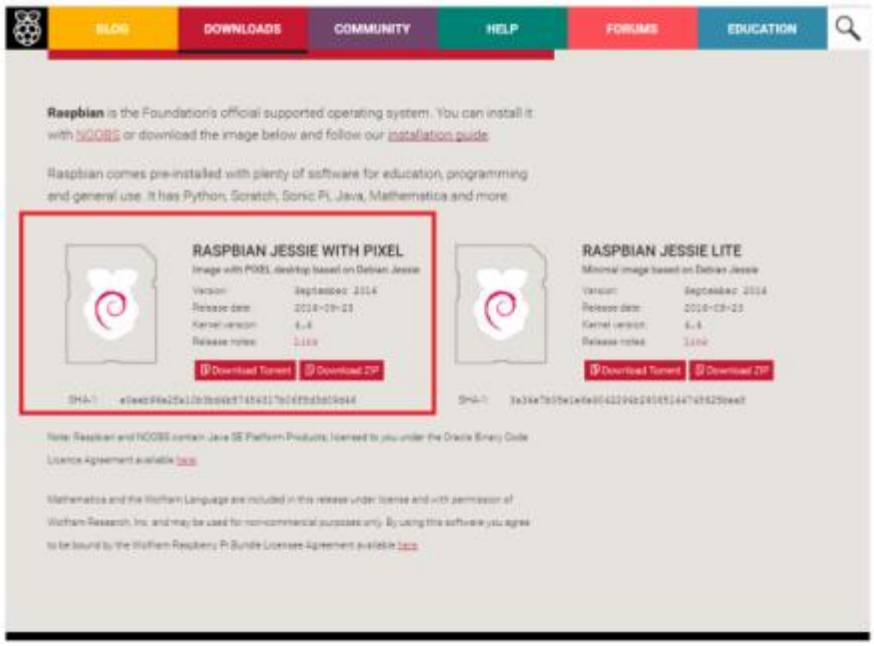

FIGURE 2. 11: TELECHARGEMENT DE RASPBIAN, POUR COMMENCER L'INSTALLATION SUR LE RASPBERRY PI

Après avoir installé et lancer Win32DiskImager, on décompresse le fichier .zip de l'image de Raspbian pour obtenir un fichier .img. On insère la carte SD dans le lecteur que l'on connecte à l'ordinateur, celle-ci doit bien être reconnue.

1. On indique ou se trouve l'image que l'on veut écrire sur la carte SD (Raspbianjessie.img).

2. On choisit la carte SD comme périphérique [J:\].

3. On appuie sur Write.

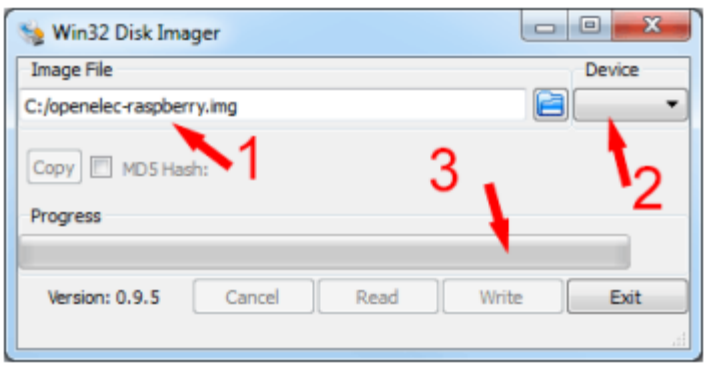

FIGURE 2. 12: : ETAPES POUR DECOMPRESSER L'IMAGE SUR LA CARTE SD.

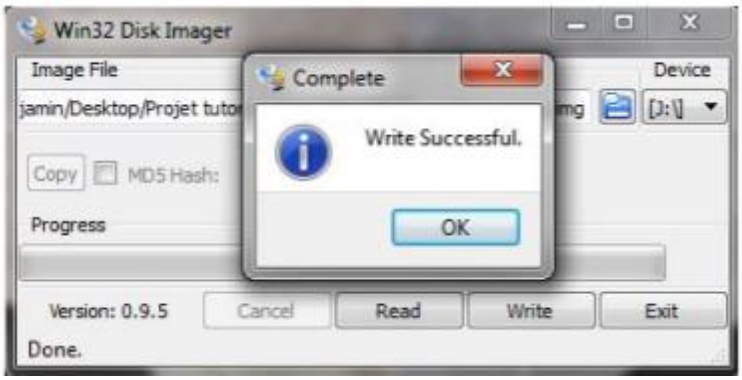

FIGURE 2. 13: ATTENDRE LA FIN DE L'ECRITURE SUR LA CARTE SD.

Nous allons maintenant insérer la carte SD et effectuer les branchements nécessaires pour démarrer le Raspberry Pi. Le Raspberry s'occupe lui-même de l'installation de Raspbian. Après le démarrage on arrive à voir sur l'écran connecté au raspberry une Interface Graphique avec déjà pas mal de fonctionnalités installées : Python 2 et 3, Java IDE, Geany, Wolfram, la suite LibreOffice, Chromium et d'autres moins utiles.

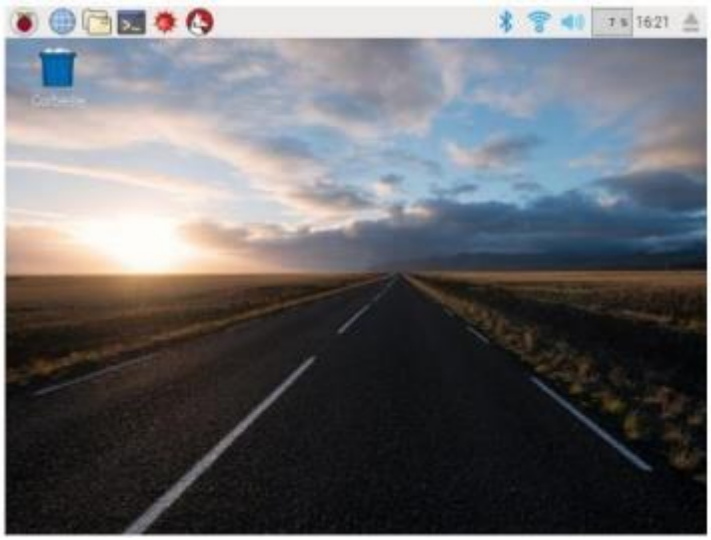

FIGURE 2. 14: BUREAU DU RASPBERRY PI 2

5. Conclusion

Dans ce chapitre, nous avons présenté les parties matérielles et logicielles dédiée à notre projet. Les composantes de notre solution ont été détaillées puis, l'application et module basée sur la technologie Arduino ont été introduits.

Chapitre 3 : Réalisation

1. Introduction

Dans cette dernière partie nous avons développé le programme de commande permettant au responsable de sécurité de contrôler tout le système sans intervention d'une manière automatique et simple. Cette phase de réalisation consiste à la concrétisation des phases précédentes au niveau technique.

2. Présentation de système

Suricata est un IDS (Intrusion Detection System) réseau basé sur des détections par signatures. Il analyse le trafic réseau afin d'y détecter des activités anormales et les tentatives d'intrusion. Un Raspberry Pi est un hôte parfait pour Suricata dans le cadre d'un petit réseau local. Afin de surveiller tous les équipements de votre réseau, l'IDS doit être en mesure d'en analyser tout le trafic. Ceci est possible grâce à l'utilisation d'un switch manageable supportant la fonction « port mirroring » permettant de dupliquer le trafic de tous les équipements et de l'envoyer vers l'IDS.

3. Architecture

L'IDS doit être capable d'analyser les trames provenant de tous les équipements de votre réseau. Pour cela il faut que tous vos équipements soient reliés au switch qui utilise la fonction port mirroring pour transmettre toutes les trames reçues des « mirrored port » vers le « analysis port ». Le Raspberry Pi sur lequel l'IDS Suricata est installé est bien entendu relié sur cet « analysis port ». Le schéma suivant résume notre système :

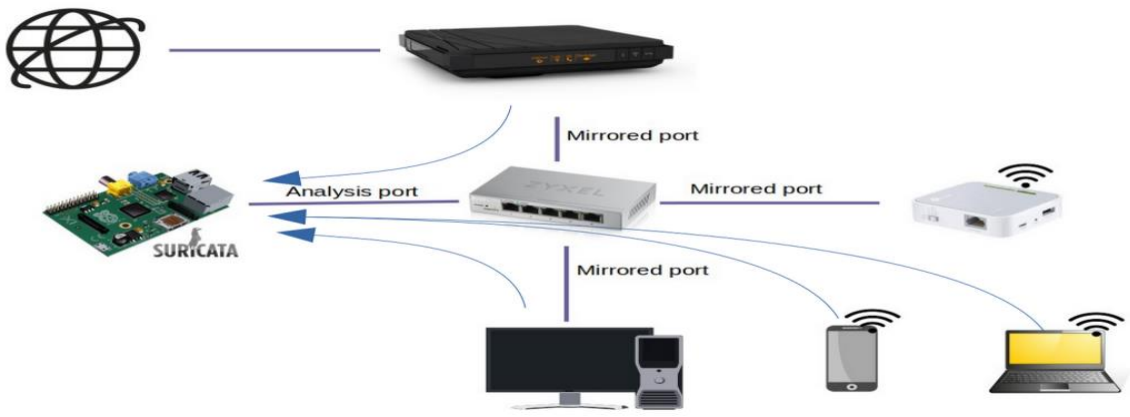

FIGURE 0-2 : ARCHITECTURE DE SYSTEME

4. Installation de Suricata sur la carte Raspberry Pi

4.1. Installation de Suricata

Nous devons installer les dépendances nécessaires :

```
sudo apt install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev make libmagic-dev libjansson-dev rustc cargo python-yaml python3-yaml liblua5.1-dev
```

Passaons au téléchargement de Suricata :

```
wget https://www.openinfosecfoundation.org/download/suricata-6.0.1.tar.gz
```

Maintenant, nous décompressons les sources :

```
tar -xvf suricata-6.0.1.tar.gz
```

On passe maintenant dans le dossier Suricata :

```
cd $HOME/suricata-6.0.1/
```

Configuration de l'installation du logiciel :

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lua
```

La Compilation de suricata :

```
make
```

L'installation de suricata :

```
sudo make install
```

Essayons de se déplacer dans le dossier suricata-update :

```
1    cd $HOME/suricata-6.0.1/suricata-update/
```

La compilation de suricata-update :

```
1    sudo python setup.py build
```

Installer suricata-update :

```
1    sudo python setup.py install
```

Se placer dans le dossier Suricata :

```
1    cd $HOME/suricata-6.0.1/
```

On doit finaliser l'installation de suricata en y incluant ses règles :

```
1    sudo make install-full
```

Mettre à jour les règles de suricata :

```
1    sudo suricata-update
```

4.2. Configuration de Suricata

Configurer suricata en éditant le fichier suricata.yaml :

```
1    sudo vi /etc/suricata/suricata.yaml
```

Modifier la variable HOME_NET afin qu'elle contienne votre réseau local, par exemple :

```
1    HOME_NET: "[192.168.0.0/24]"
```

4.3. Utilisation de Suricata

Lancer suricata avec la commande suivante :

```
1 sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules
```

-c <chemin> : fichier de configuration à utiliser

-i <interface> : interface Ethernet à surveiller

-S <chemin> : fichier contenant les règles à utiliser

4.4. Test de Suricata

Afin de tester le bon fonctionnement de suricata, il est utile de rajouter une règle qui affiche un avertissement à chaque réception d'un ICMP Echo (ping). Il faudra supprimer cette règle après ce test.

Ajouter la règle suivante dans ***/var/lib/suricata/rules/suricata.rules***

```
1 alert icmp any any -&gt; any any (msg: "ICMP Packet found"; sid: 1; rev: 1;)
```

Afficher le contenu du fichier de log :

```
1 sudo tail -f /var/log/suricata/fast.log
```

5. Optimisation de Suricata sur la carte Raspberry Pi

Suricata peut nécessiter quelques optimisations afin de fonctionner de façon optimale sur votre réseau. Cela dépend bien entendu du nombre d'équipements à surveiller et du trafic généré.

5.1. Éviter la perte de paquets

On doit Vérifier que la variable **capture.kernel_drops** dans le fichier ***/var/log/suricata/stats.log*** ne soit pas trop élevée. Idéalement elle doit rester à 0 et donc ne pas être affichée dans la liste des compteurs.

Le contenu du fichier mentionnée ci-dessus est dans la figure suivante :

```
-------------------------------------------------------------------
Date: 1/28/2021 -- 18:29:22 (uptime: 0d, 03h 02m 49s)
-------------------------------------------------------------------
Counter                       | TM Name         | Value
-------------------------------------------------------------------
capture.kernel_packets        | Total           | 2310188
capture.kernel_drops          | Total           | 21617
decoder.pkts                  | Total           | 2288600
decoder.bytes                 | Total           | 1882135284
decoder.ipv4                  | Total           | 2272391
decoder.ipv6                  | Total           | 24
decoder.ethernet              | Total           | 2288600
decoder.tcp                   | Total           | 1320915
```

FIGURE 0-3 : CONTENU DE FICHIER « /VAR/LOG/SURICATA/STATS.LOG »

Dans le cas ci-dessus, 21617 paquets sur 2310188 ont été perdus, soit environ 1 %. C'est acceptable mais cette perte peut être évitée.

On peut aussi augmenter la valeur de la variable « **ring-size** » dans le fichier de configuration « ***/etc/suricata/suricata.yaml***« . Attention, il faut bien entendu supprimer le « # » devant la variable dans le fichier ***suricata.yaml***. Cette modification est en général suffisante pour éviter de perdre des paquets.

Modifier la valeur de **ring-size** en changeant la ligne suivante dans le fichier ***/etc/suricata/suricata.yaml*** :

```
#ring-size: 2048
```

Par

```
1          ring-size: 30000
```

Après avoir augmenté cette variable à 30000, je n'observe plus de perte de paquets, même avec 7.8 millions de paquets reçus.

```
-------------------------------------------------------------------
Date: 1/31/2021 -- 17:11:29 (uptime: 0d, 20h 49m 24s)
-------------------------------------------------------------------
Counter                       | TM Name         | Value
-------------------------------------------------------------------
capture.kernel_packets        | Total           | 7885374
decoder.pkts                  | Total           | 7885383
decoder.bytes                 | Total           | 7978255434
```

FIGURE 0-4 : CONTENU DE FICHIER « /VAR/LOG/SURICATA/STATS.LOG » (1)

Bibliographiques

[1]. ZERKOUK Meriem. Thèse de doctorat. «Modèles de contrôle d'accès dynamiques» USTOMB.2015. Faculté des Mathématiques et Informatique.

[2]. L'agriculture de précision. Bars, Philippe Zwaenepoel & Jean-Michel Le. 1997.

[3]. **Historique.** [En ligne] https://iot.goffinet.org/iot_internet_des_objets.html.

[4]. "Internet of Things– From Research and Innovation to Market Deployment", river publishers' series in communications. Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium,. 2014.

[5]. **Plouin, N. C. Guillaume.** «Modèles d'architectures de l'Internet des Objets,». *«Modèles d'architectures de l'Internet des Objets,».* [En ligne] https://blog.octo.com/.

[6]. N. C. Guillaume Plouin, «Modèles d'architectures de l'Internet des Objets,» [En ligne]. Available: https://blog.octo.com/.

[7]. «L'IoT au travail aujourd'hui,» [En ligne]. Available: https://www.intel.fr/.

[8]. https://codevele.com/tutorials/arduino/how-to-use-a-buzzer-arduino-tutorial.html

[9]. Carte de développement W5100 (Arduino Ethernet Shield). *synotec.* [En ligne] https://synotec.tn/.