وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

Année : 2019

Faculté: Sciences de l'Ingéniorat
Département: Electronique

MEMOIRE
Présenté en vue de l'obtention du diplôme de : MASTER

Intitulé :
Système de surveillance et contrôle d'accès à base de la technologie RFID

Domaine : Sciences et Technologie
Filière : Automatique
Spécialité: Automatique et Informatique Industrielle

Par :
HACENE CHAOUCHE HMAIDA

DEVANT Le JURY

Président :	**Pr. R. Lakel**	**Grade : Professeur**	**UBM Annaba**
Directeur de mémoire:	**Dr. M. Saadi**	**Grade : Professeur**	**UBM Annaba**
Examinateurs 1 :	**Pr. N. guerssi**	**Grade : Professeur**	**UBM Annaba**
Examinateurs 2 :	**Pr. N. debbach**	**Grade : MCA**	**UBM Annaba**

Résumée en français :

Le système conçu et réalisé de sécurité de contrôle d'accès est basé sur l'identification par radio fréquence RFID avec la technologie LoT, Permet de surveiller et d'empêcher l'accès non autorisé aux environnements contrôlés, ainsi que la sauvegarde des traces d'accès. Pour réaliser notre système, nous avons recouru pour la partie matérielle à : un module RFID MFRC522 fonctionnant à 13 MHz, un microcontrôleur (Node MCU v3 doté d'un Soc wifi ESP8266) programmé pour envoyer des signaux de contrôle, serrure électrique 12v DC, relais, buzzer, ,écran d'affichage OLED, pour la partie logicielle : le code pour le microcontrôleur a été écrit en langage C++ pour Arduino , débuggé et compilé en utilisant L'IDE Arduino. La simulation matérielle a été réalisée en utilisant le logiciel Proteus professionnel 8.

Le domaine applicatif est tellement vaste que toutes les applications ne peuvent être citée. Nous citons à titre non restrictif, la sécurité des maisons, des organisation et terminaux automobiles.

Des améliorations futures peuvent être apportées à ce travail afin de le rendre plus novateur comme ajouter un système de reconnaissance faciale ainsi qu'une authentification par reconnaissance d'iris, construire un PCB évolué comportant tous les composants utilisés, organisés d'une manière plus esthétique, réduire le cout d'entretien, etc

Résumé en anglais:

The designed and realized access control security system is based on RFID RFID identification with LoT technology, allows to monitor and prevent unauthorized access to controlled environments, as well as the safeguarding of traces of 'access. To realize our system, we resorted for the hardware part to: a RFID module MFRC522 operating at 13 MHz, a microcontroller (Node MCU v3 equipped with a Soc wifi ESP8266) programmed to send control signals, electric lock 12v DC, relay, buzzer,, OLED display screen, for the software part: the code for the microcontroller was written in C ++ for Arduino, debugged and compiled using the Arduino IDE. The hardware simulation was performed using the professional Proteus software 8.

The application domain is so vast that not all applications can be cited. We quote in a nonrestrictive way, the security of the houses, the organizations and the car terminals.

Future improvements can be made to this work in order to make it more innovative like adding a face recognition system as well as an iris recognition authentication, build an advanced PCB with all the components used, organized in a more aesthetic way , reduce the cost of maintenance, etc.

Resumé en arabe:

يعتمد نظام أمان التحكم في الوصول المصمم والمحقق على تحديد RFID RFID مع تقنية LoT ، ويسمح بمراقبة ومنع الوصول غير المصرح به إلى البيئات التي يتم التحكم فيها ، بالإضافة إلى حماية آثار الوصول. لتحقيق نظامنا ، لجأنا إلى جزء الأجهزة إلى: وحدة RFID MFRC522 تعمل بسرعة 13 ميجاهرتز ، متحكم دقيق (Node MCU v3 مجهز بـ Soc wifi ESP8266) مبرمج لإرسال إشارات التحكم ، القفل الكهربائي 12 v DC، relay، buzzer ،، ،، شاشة عرض OLED، لجزء البرنامج: تمت كتابة رمز متحكم في C ++ لـ Arduino، تم تصحيحه وتجميعه باستخدام Arduino IDE. تم إجراء محاكاة الأجهزة باستخدام برنامج Proteus المحترف 8.

مجال التطبيق واسع جدًا بحيث لا يمكن ذكر جميع التطبيقات. نحن نقتبس بطريقة غير مقيدة ، وأمن المنازل والمنظمات ومحطات السيارات.

يمكن إجراء تحسينات مستقبلية لهذا العمل من أجل جعله أكثر إبداعًا مثل إضافة نظام التعرف على الوجوه وكذلك مصادقة التعرف على قزحية العين ، وبناء PCB متقدم مع جميع المكونات المستخدمة ، المنظمة بطريقة جمالية أكثر ، تقليل تكلفة الصيانة ، الخ

Dédicaces

A mes chers parents, pour tous les sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chers frères, Nabil Mohammed, Iskander, Med Samy pour leurs appuis et leur encouragement,

A mes chers amis, Haythem, Haythem B, Mohcene, Adel. Oussama, Abdenour, pour leur soutien permanent,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Remercîments

Tout d'abord, je tiens à remercier dieux de m'avoir donné la santé, la volonté et la patience pour réaliser ce travail.

Mes remerciements vont à Dr Mohamed nacer saadi mon

Encadreur qui a guidé de ses précieux conseils et suggestions, et la confiance qu'il m'a témoigné et tout au long de ce travail.

Je tiens à gratifier aussi les membres de jury pour l'intérêt qu'ils ont porté à moi en acceptant d'examiner mon travail.

J'adresse aussi mes remercîments à mes chers frères mohcéne et Imed et Ayoub pour leur encouragement et leur aide.

J'adresse mes sincères sentiments de gratitude et de reconnaissance à toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Liste des abréviations :

RFID	Radio frequency identification
GSM	Global system for mobile
GPRS	General packet radio service
HTTP	Hyper text transfer protocol
HF	High frequency
I2C	Inter Integrated Circuit
LoT	Internet of Things
LF	Low frequency
MCU	Micro Controller Unit
NFC	Near Field Communication
OLED	Organic Light Emitting Diodes
RF	Radio Frequency
SPI	Serial Peripheral Interface
SHF	Super High Frequency
USB	Universal Serial Bus
UHF	Ultra High Frequency
UID	Unique Identifier Number
UART	Universal Asynchronous Receiver Transmitter

Liste des figures :

SOMMAIRE :

1. Introduction générale :

Insérer une clé pour démarrer un véhicule, badger pour accéder à un bâtiment ou une salle, valider un titre de transport dans le bus ou le métro sont des gestes entrés dans le quotidien de bon nombre d'entre nous. On utilise, sans en être toujours conscient, des technologies de capture automatique de données basées sur les ondes et rayonnements radiofréquence.

La RFID pour <<Radio Frequency Identification>> vient remplacer des technologies en apportant des solutions efficaces dans différents domaines, elle permet de tracer les produits et les animaux, d'identifier des personnes, de sécuriser des lieux ... Les caractéristiques de cette technologie sont : la lecture distante et même sans ligne de vue directe, la rapidité, l'unicité des ID des tags...

En effet la Radio-Identification ou la RFID est l'annonce d'une mutation radicale dans l'organisation du commerce, du transport, de la sécurité et de la surveillance.

Le domaine applicatif est tellement vaste que toutes les applications ne peuvent être citées. cette technologie s'est vue aussi combinée avec d'autre : RFID-GSM, RFID-LoT, etc.

1.1 Motivation et problématique :

La sécurité est l'un des aspects les plus importants pour les entreprises. Le système de contrôle d'accès régit l'accès aux bâtiments ou aux zones nécessitant une protection selon les principes « qui, quand, où ? » et, éventuellement, « avec qui ». Un système de contrôle d'accès est un outil électronique responsable de contrôler les accès et vérifiant automatiquement si une personne a les autorisations pour accéder à un bâtiment, une zone ou une pièce déterminée. La durée de ces autorisations est également définie. Celle-ci peuvent être unique, limitée dans le temps ou illimitée. Un système de contrôle d'accès augmente sensiblement la sécurité et soutient les processus de l'entreprise.

Pour développer notre système de contrôle et de surveillance d'accès, on a besoin d'étudier deux techniques : la technologie RFID et un verrouillage de porte connecté au réseau. Pour développer notre serrure connectée on combinera ces deux techniques.

1.2 Objectifs :

L'objectif principal de ce projet et de développer un système de contrôle et de surveillance d'accès connecté au réseau.

Le projet contient deux parties :

- La première partie concerne le module RFID er son raccordement avec le microcontrôleur
- La deuxième partie concerne la communication entre le microcontrôleur et le serveur

1.3 Structure du mémoire :

Ce mémoire est organisé en quatre chapitres. L'objectif de premier chapitre est de présenter les généralités sur les technologies utilisées. Le deuxième montre des systèmes a réalisés à base de la technologie RFID et présenter les méthodes et les outils réalisés dans ce domaine. Le troisième chapitre concentre sur les méthodes de conception du système de contrôle et surveillance d'accès. Le quatrième chapitre explique le hardware et présente le software qu'on a utilisé pour réaliser notre système et une conclusion.

1.Introduction

Dans ce premier chapitre, on va introduire des concepts utiles à savoir pour mieux comprendre le fonctionnement de notre système ainsi qu'une présentation des technologies utilisées dans la réalisation du système de surveillance et contrôle d'accès.

2. Introduction à la technologie RFID

2.1 Définition :

La radio-identification, plus souvent désignée par le sigle RFID ("Radio Frequency Identification") est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés radio-étiquettes ("RFID Tag").

2.2 De I 'identification à la RFID

L'identification électronique se divise en deux branches :

- L'identification à contact
- L'identification sans contact.

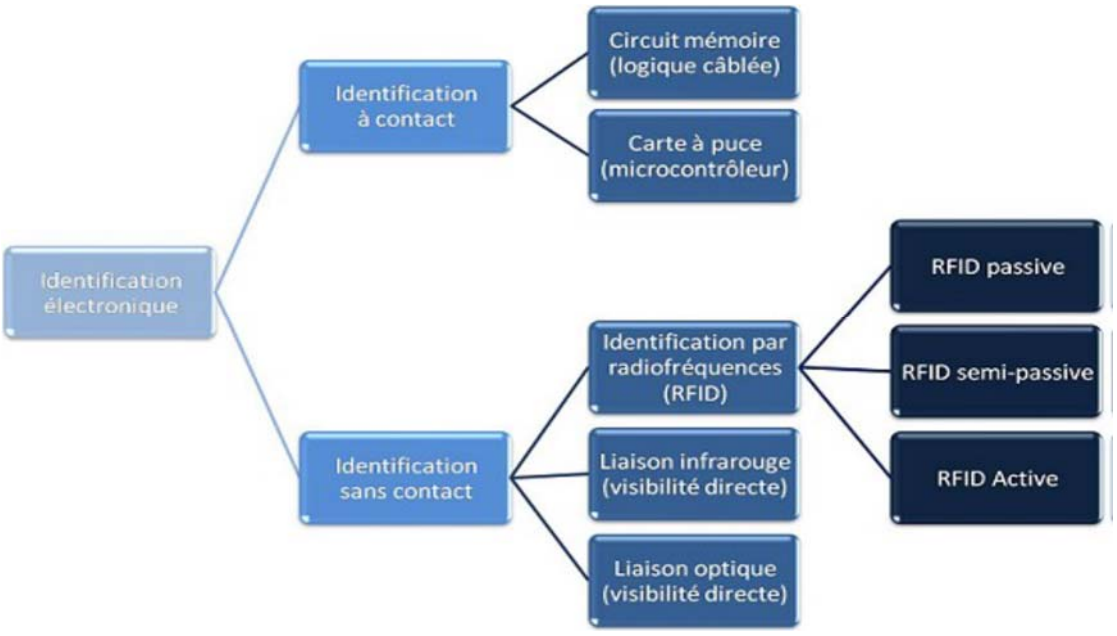

Figure 1 : les branches d'identification électronique

2.2.1 Identification à contact :

Il s'agit de dispositifs comportant un circuit électronique dont l'alimentation et la communication Sont assurées par des contacts électriques. Les deux principaux exemples d'identification à contact Sont :

• Les circuits « mémoire » : ils comportent des fonctions mémoire embarqués sur des modules de formes et de tailles variées.

• Les cartes à puces : Les exemples de cartes à puces les plus connus sont les cartes bancaires, ou encore la carte SIM (Subscriber Identity Module).

2.2.2 Identification sans contact :

On peut décomposer les identifications sans contacts en trois sous-branches principales :

• La vision optique : ce type de liaison nécessite une vision directe entre l'identifiant et le

Lecteur (laser, camera CCD...).

La technologie la plus répandue est le code à barre linéaire et les codes 2D (PDF417, QR Code, etc.). La technologie OCR (Optical Character Recognition) est également largement utilisée (scan MRZ (Machine Readable Zone) sur les Passeports ou Carte National d'Identité).

• La liaison infrarouge : Ce type de liaison assure un grand débit d'information, une grande directivité qu'une bonne distance de fonctionnement. Ces systèmes nécessitent également une visibilité directe.

• Les liaisons Radiofréquences : Ce type de liaison permet la communication entre l'identifiant et un interrogateur, sans nécessité de visibilité directe. De plus, il est également possible de gérer la présence simultanée de plusieurs identifiants dans le champ d'action du lecteur (anticollisions).

2.3 Classification des tags RFID

2.3.1 Les tags passifs : sont donc les tags RFID les plus économiques et les plus généralement utilisés dans les applications de la chaîne logistique. A la différence des tags actifs, ils ne sont pas équipés de pile interne, car ils tirent leur énergie des lecteurs RFID. Le lecteur RFID envoie des ondes électromagnétiques à l'antenne du tag, qui va réagir (se « réveiller ») et renvoyer un signal au lecteur en utilisant l'énergie de ces ondes.

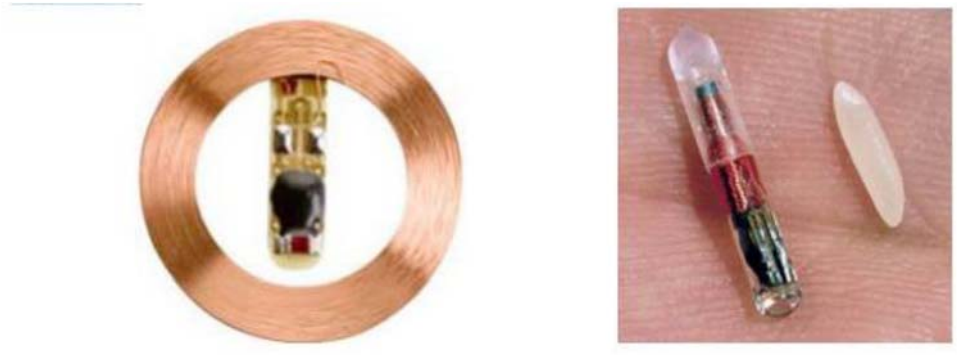

Figure2 : Tags à couplage inductif

2.3.2 Les tags actifs : utilisent leur propre énergie pour émettre leurs ondes, en utilisant une pile interne. Ils peuvent ainsi avoir une très longue distance de lecture. Ils sont plus onéreux que les tags passifs et sont donc généralement utilisés pour tracer des articles de valeur.

2.3.3 Les tags semi-passifs : petits et légers, sont des tags intermédiaires entre les tags actifs et les tags passifs. Ils utilisent généralement une pile comme source d'énergie (comme les tags actifs), mais ils peuvent également transmettre des données en utilisant l'énergie générée par les ondes des lecteurs RFID (comme les tags passifs) [2].

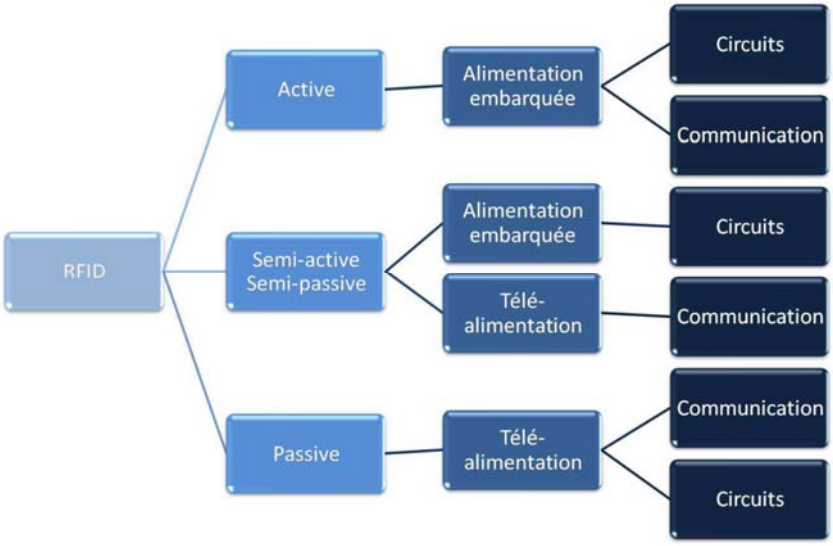

Figure3 : Classification des tags RFID

2.4 Caractéristiques du tag passif

Le tag passif est moins couteux et peut être de plus petite dimension, ils sont de très loin les plus utilisés sur le marché actuel. Leur prix unitaire varie entre quelques centimes d'euros selon leur fréquence, leur forme, leur taille et surtout leur packaging….

Voici les caractéristiques générales des transpondeurs passifs actuels :

Fréquence	125 et 134,2 kHz LF	13,56 MHz HF	868 à 915 MHz UHF	2,45 et 5,8 GHz SHF
Portée typique max	0,5 m	1 m	3 à 6 m	1 m
Caractéristiques générales	-Relativement cher même par gros volumes - L'antenne nécessite un nombre de tours important - Faible dégradation des performances en milieu métallique ou liquide	-Moins cher que les tags LF - Bien adapté aux applications qui ne demande pas de lire beaucoup de tags à grande distance -Fréquence unique dans le monde	-En gros volume, les tags UHF sont moins chers que les tags HF et LF - Adapté à la lecture en volume à longue distance - Performances dégradées par rapport à la HF en milieu métallique ou aqueux	-Performances similaires à l'UHF - Très forte sensibilité aux métaux et liquides - Liaison lecteur/tag plus directive que pour les fréquences plus basses
Principales Normes	ISO 14223/1 ISO 18000-2	ISO 14443 ISO 15693 ISO 18000-3	ISO 18000-6	ISO 18000-4

Figure4 : Les caractéristiques d'un système RFID

2.5 Fonctionnement d'un système RFID

2.5.1 Les composants d'un système RFID

Un système complet utilisant la technologie RFID est composé des éléments suivants :

- **Un transpondeur** : ou étiquette qui est programmé avec des données identifiant l'objet sur lequel il sera placé.
- **Une antenne** : qui est généralement intégrée au lecteur RFID et à l'étiquette RFID. Elle permet d'activer les tags afin de recevoir des données et d'en transmettre les informations.
- **Un lecteur** : fixe ou portable, qui est un élément essentiel à l'utilisation de la RFID. Il transmet à travers des ondes-radio l'Energie au tag RFID, une requête d'informations

est alors émise aux étiquettes RFID situées dans son champ magnétique, puis il réceptionne les réponses et les transmet aux applications concernées.

- **Le logiciel RFID** : ou middleware RFID, est le cerveau de la chaîne RFID. Il permet de transformer les données brutes émises par la puce RFID en informations compréhensibles, il est bien sûr géré par un ordinateur [1].

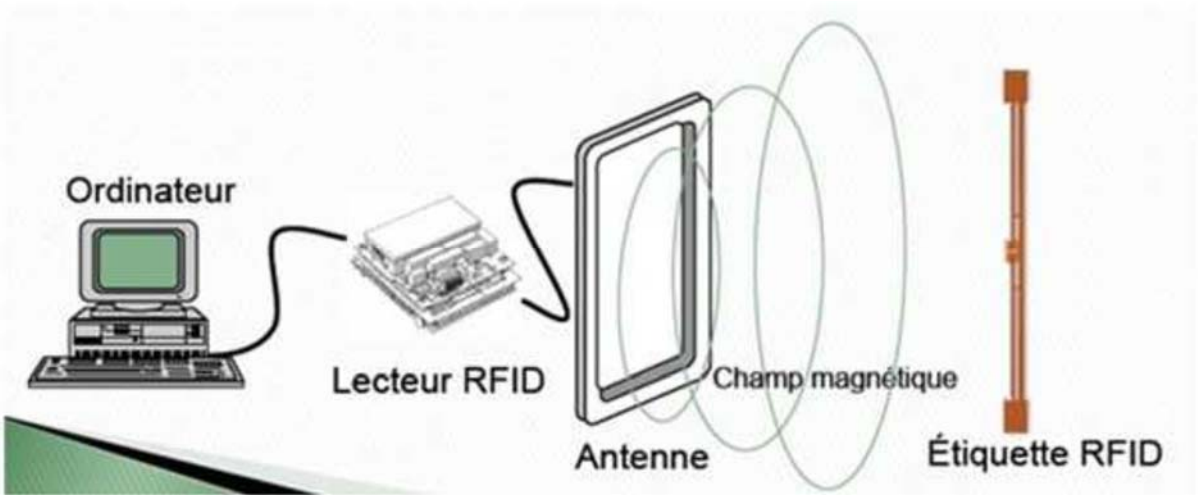

Figure5 : Illustration d'un système RFID

2.5.2Principe de fonctionnement :

Système RFID : un système RFID se compose de transpondeur (étiquette, marqueurs, tags, identifiants…) et d'un ou plusieurs interrogateurs (coupleurs, base station…).

Lorsque le lecteur composé d'un bobinage est alimenté en tension, il génère un champ magnétique et lorsque un tag composé également d'un bobinage s'en approche par un effet électromagnétique cela génère un courant électrique et donc une différence de potentiel qui permet une puce électronique dans le tag d'être alimentée en tension a partir de cet instant le lecteur et la puce utilise leurs antennes pour échanger des données a très courte distance dans le numéro d'identification du tag sachez également qu'un tag RFID contient un peu plus qu'un numéro d'identification mais également une mémoire de quelque ko.

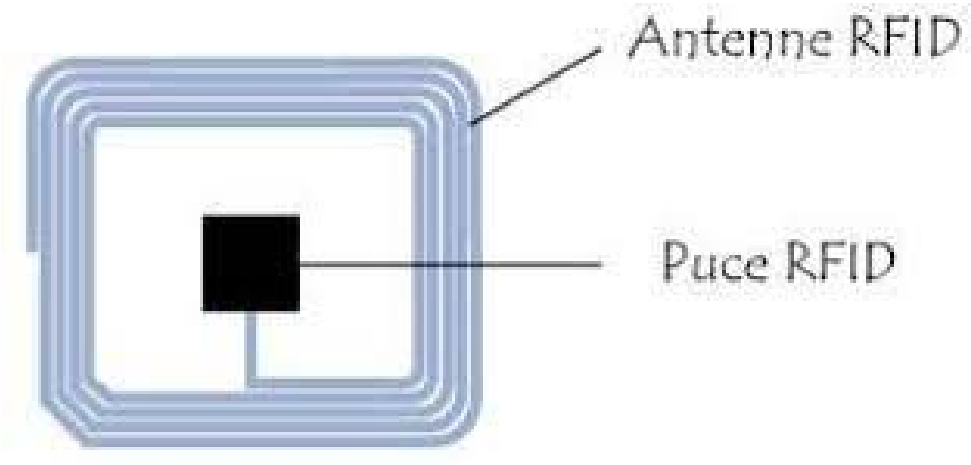

Figure7 : Structure du tag RFID

2.6 Les gammes de fréquences RFID

2.6.1 La RFID dans le spectre radio :

Le système RFID utilise le canal hertzien pour ses communications. L'utilisation de ressources radio est soumise à autorisation et suit des règlements nationaux ou internationaux, on les classes ainsi en quatre catégories :

- BF : pour des fréquences inferieures à 135 MHz
- HF : pour des fréquences qui avoisinent les 135 MHz
- UHF : pour des fréquences autour de 434 MHz, de 869-915 MHz, 2,5 GHz
- SHF ; pour des fréquences aux alentours de 2,5 GHz

Voici un aperçu des fréquences de la RFID dans le spectre radio :

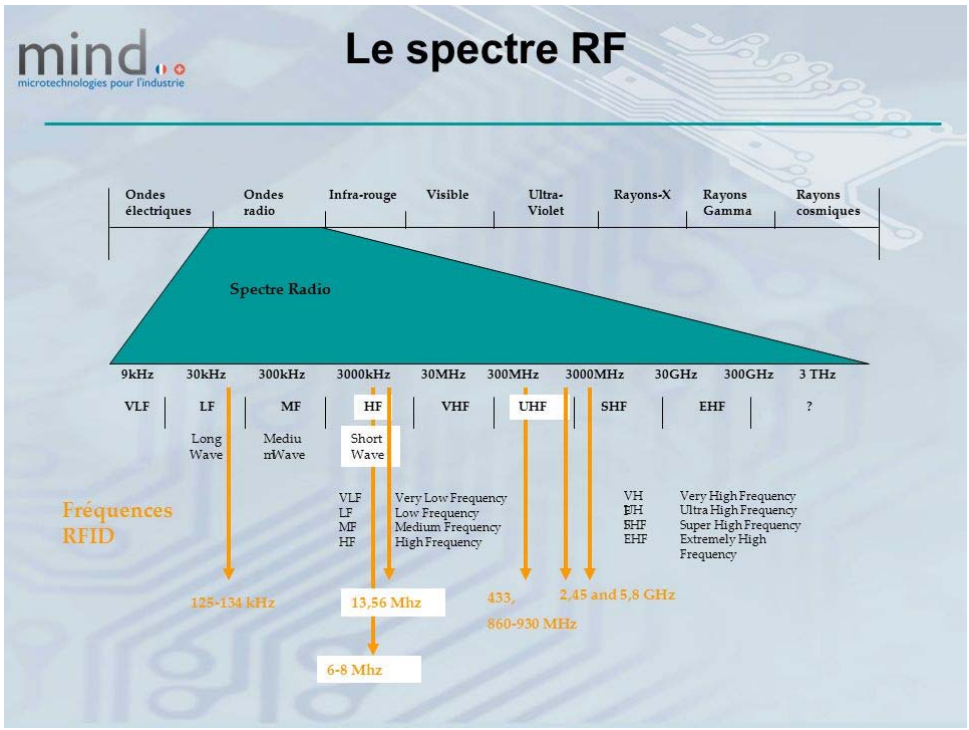

Figure8 : Les fréquences RFID dans le spectre radio

Selon l'étude « RFID Forecasts, Playersand Opporunities 2014-2024 » d'ID TechEx, l'estimation du nombre de tags RFID passifs qui seront vendus sur le marché en 2020, toutes applications et marchés confondus sont présentés ci-dessous :

- LF : 1308 millions (646.5 en 2013)
- HF : 5904 millions (2182 en 2013)
- UHF : 30000 millions (3079 en 2013)[22] .

2.7 Applications de la RFID

La RFID est actuellement une technologie en plein essor et qui se développe dans des domaines de plus en plus variés ; Sécurité, transport, logistique, fidélisation client, paiement, santé, etc. Son utilisation varie selon la fréquence (LF, HF, UHF) où chaque plage de fréquence répond à une norme qui décrit une série de technologies RFID (ISO 18000-x) comme nous pouvons le voir dans les exemples suivants :

Fréquence	Applications
<135 kHz	-Tri des déchets, -Identification animale (134,2 kHz), -Système d'alarme, surveillance des arbres de Paris…
13,56 MHz	-Cartes à puce sans contact, cartes de transport… -Réservation de billets d'avion, manutention des bagages -Forfait de station de ski. . .
443 et 900MHz	-Traçage de palettes, de conteneurs, -Télécommandes d'ouverture centralisée
2,45 et 5,8 GHz	-Télépéage, -Délivrance automatique du carburant dans les stations-service.

Figure9 : Les applications de la RFID suivant la fréquence

3. Internet des objets :

3.1 Définition :

L'internet des objets (Ido) est une infrastructure dynamique d'un réseau global qui permet d'interconnecter des objets (physiques ou virtuels) grâce aux technologies de l'information et de La communication interopérable.

D'un point de vue conceptuel, l'Internet des objets affecte, à chaque objet une identification unique sous forme d'une étiquette lisible par des dispositifs mobiles sans fil, afin de pouvoir de communiquer les uns avec les autres. Ce réseau crée une passerelle entre le monde physique et le monde virtuel. D'un point de vue technique, l'Ido consiste l'identification numérique directe et normalisée (adresse IP, protocole http...) d'un objet physique grâce à un système de communication sans (puce RFID, Bluetooth ou WIFI). [3] .

Figure10 ; Les objets de la vie quotidienne connectés entre eux

3.2 L'évolution de l'écosystème de l'internet des objets :

Les premiers objets connectés n'apparaissent que dans les années 1990. Il s'agit de grille-pain,

Machines à café ou autres objets du quotidien. En 2000, le fabricant coréen LG est le premier industriel à parler sérieusement d'un appareil _électroménager relié à internet, Les années 2000 verront les premières expérimentations d'appareils connectés à Internet. Ils l'utilisent notamment pour consulter des informations de manière automatique.

En 2003, la population mondiale s'élevait _a environ 6,3 milliards d'individus et 500 millions d'appareils étaient connectés à Internet. Le résultat de la division du nombre d'appareils par la population mondiale (0,08) montre qu'il y avait moins d'appareil connecté par personne. Selon la définition de Cisco IBSG, l'Ido n'existait pas encore en 2003 car le nombre d'objets connectes était faible.

En raison de l'explosion des Smartphones et des tablettes, le nombre d'appareils connectés à Internet a atteint 12,5 milliards en 2010, alors que la population mondiale était de 6,8 milliards. C'est ainsi que le nombre d'appareils connectés par personne est devenu supérieur à 1 (1,84 pour être exact) pour la première fois de l'histoire.

En affinant ces chiffres, Cisco IBSG a situé l'apparition de l'Ido entre 2008 et 2009. En ce qui concerne l'avenir, Cisco IBSG estime que 50 milliards d'appareils seront connectes à Internet d'ici à 2020. Il est important de noter que ces estimations ne tiennent pas compte des progrès rapides d'Internet ni des avancées technologiques, mais reposent sur les faits avérés a l'heure actuelle.

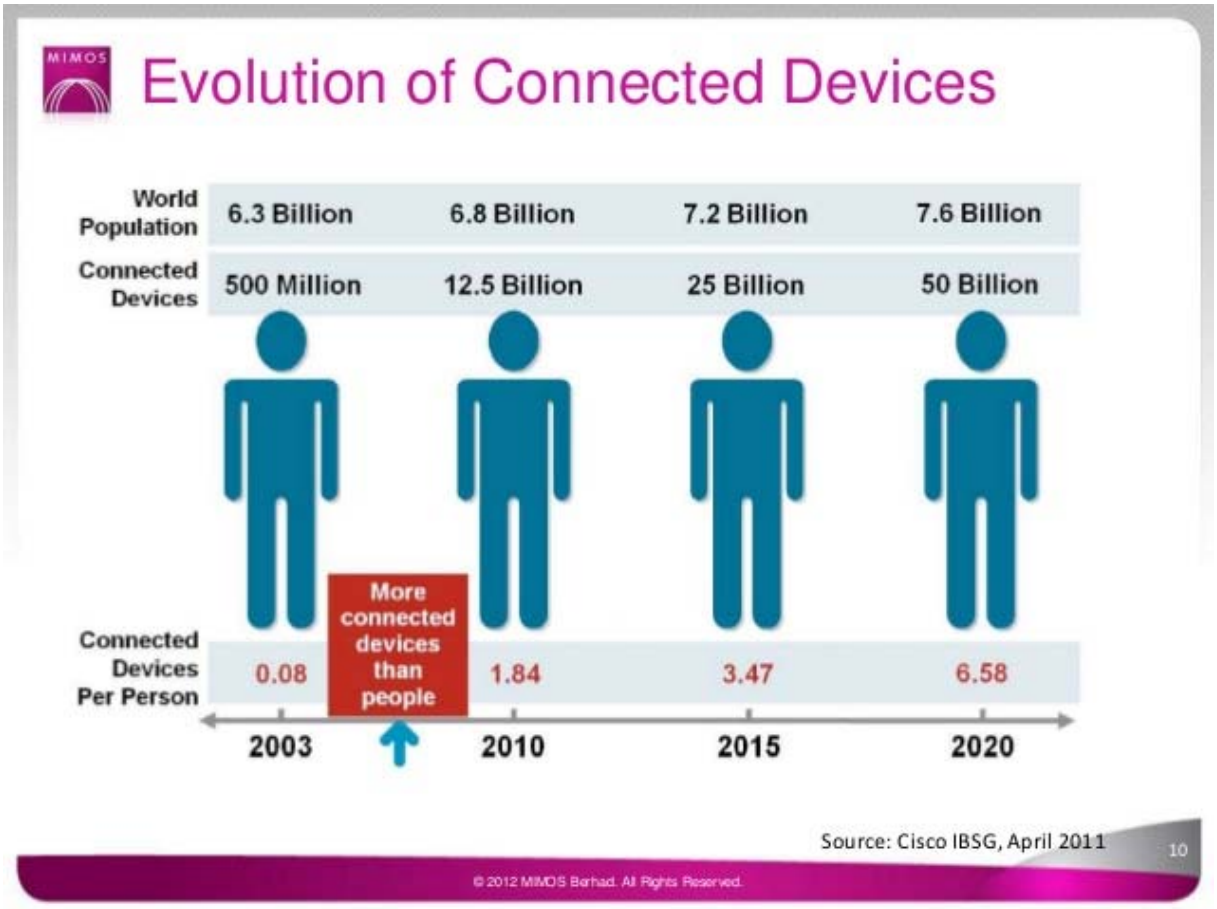

Figure11 : L'internet des objets est apparu entre 2008 et 2009

3.3 L'Internet des objets : applications et futur

Les objets connectés produisent de grandes quantités de données dont le stockage et le traitement entrent dans le cadre de ce que l'on appelle les big data. En logistique, il peut s'agir de capteurs qui servent à la traçabilité des biens pour la gestion des stocks et les acheminements. Dans le domaine de l'environnement, il est question de capteurs surveillant la qualité de l'air, la température, le niveau sonore, l'état d'un bâtiment, etc.

En domotique, l'IdO recouvre tous les appareils électroménagers communicants, les capteurs (thermostat, détecteurs de fumée, de présence...), les compteurs intelligents et systèmes de sécurité connectés des appareils de type box domotique.

Le phénomène IdO est également très visible dans le domaine de la santé et du bien-être avec le développement des montres connectées, des bracelets connectés et d'autres capteurs surveillant des constantes vitales. Selon diverses projections (cf. Cisco et le cabinet Gartner), le nombre d'objets connectés devrait largement augmenter au fil des ans.

3.4 Domaine d'application :

L'utilisation de la technologie de l'Internet des objets est tellement vaste qu'on ne peut tout citer :

En logistique :

- Utilisation des puces RFID.
- Permet de rendre la marchandise « intelligente » /traçable.
- Entrepôts entiers entièrement automatisés (Amazon).

Dans le domaine pharmaceutique :

- Puces biodégradables évitant les contrefaçons.
- Automatisation de la préparation des ordonnances.

Dans le domaine de la domotique :

- Piloter ses ouvrants.
- Contrôler les chauffages.
- Contrôler l'ouverture des portes.

Dans le domaine d'Energie :

- L'Ido propose des possibilités de gestion en temps réel pour une distribution et ingestion efficaces de l'Energie, comme les réseaux électriques intelligents (smart grid). Cela permet d'avoir le contrôle de la consommation d'Energie et la détection des fraudes.

Dans le domaine de transport :

- Des voitures connectées aux systèmes de transport/logistique intelligents, l'Ido peut sauver des vies, réduire le trac, minimiser l'impact des véhicules sur l'environnement et renforcer la sécurité routière.

Dans le domaine de l'industrie :

- La technologie Ido permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production, d'améliorer la sécurité des employés, facilite la lutte contre la contrefaçon, la fraude et assure un suivi total des produits.

Figure12 : Domotique et IOT

4 Les protocoles réseaux :

4.1 Qu'est-ce qu'un protocole ?

Un protocole est une méthode standard qui permet la communication entre des processus, c'est-à-dire un ensemble des règles et des procédures à respecter pour émettre et recevoir des données sur un réseau.

4.2 Le protocole http :

4.2.1 Définition :

Le protocole **HTTP** (HyperText Transfer Protocol) est le protocole le plus utilisé sur Internet depuis 1990.

Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée **URL** entre un navigateur (le client) et un serveur Web.[4] .

4.2.2 Communication client/ serveur :

La communication entre le navigateur et le serveur se fait en deux temps :

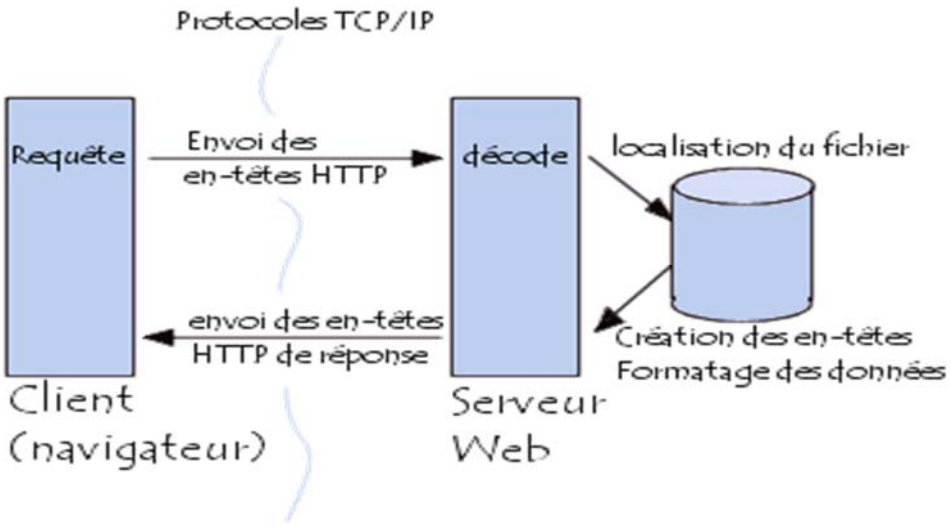

Figure13 : Communication client-serveur avec le protocole http

- Le navigateur effectue une **requête HTTP**
- Le serveur traite la requête puis envoie une **réponse http**

4.2.3Requête HTTP

Une requête HTTP est un ensemble de lignes envoyé au serveur par le navigateur. Elle comprend :

- Une ligne de requête : c'est une ligne précisant le type de document demandé, la méthode qui doit être appliquée, et la version du protocole utilisée. La ligne comprend trois éléments devant être séparés par un espace :
  - La méthode
  - L'URL
  - La version du protocole utilisé par le client (généralement *HTTP/1.0*)
- Les champs d'en-tête de la requête : il s'agit d'un ensemble de lignes facultatives permettant de donner des informations supplémentaires sur la requête et/ou le client (Navigateur, système d'exploitation, ...). Chacune de ces lignes est composée d'un nom qualifiant le type d'en tête, suivi de deux points (:) et de la valeur de l'en-tête
- Le corps de la requête : c'est un ensemble de lignes optionnelles devant être séparées des lignes précédentes par une ligne vide et permettant par exemple un envoi de données par une commande POST lors de l'envoi de données au serveur par un formulaire.

4.2.4 Réponse http

Une réponse HTTP est un ensemble de lignes envoyées au navigateur par le serveur. Elle comprend :

- Une ligne de statut : c'est une ligne précisant la version du protocole utilisé et l'état du traitement de la requête à l'aide d'un code et d'un texte explicatif. La ligne comprend trois éléments devant être séparés par un espace :
  - La version du protocole utilisé
  - Le code de statut
  - La signification du code
- Les champs d'en-tête de la réponse : il s'agit d'un ensemble de lignes facultatives permettant de donner des informations supplémentaires sur la réponse et/ou le serveur. Chacune de ces lignes est composée d'un nom qualifiant le type d'en tête, suivi de deux points (:) et de la valeur de l'en-tête
- Le corps de la réponse : il contient le document demandé.

5. Le microcontrôleur :

5.1 Définition :

Un microcontrôleur est un circuit intégré qui réunit :

- Un processeur,
- Des mémoires,
- Des interfaces,
- Des périphériques,

Les microcontrôleurs se caractérisent par un plus haut degré d'intégration, une plus faible consommation électrique, une vitesse de fonctionnement plus faible et un coût réduit par rapport aux microprocesseur polyvalents utilisés dans les ordinateurs personnels Depuis l'avènement de l'informatique embarquée, on le retrouve partout (automatisation, industrie, les appareils de bureau……) [5].

5.2 Les caractéristiques principales d'un microcontrôleur :

Les microcontrôleurs sont des composants qui permet la gestion des cartes, ils sont caractérisés par :

- De nombreux périphériques d'E/S

- Une mémoire de programme
- Une mémoire vive (en général de type SRAM)
- Eventuellement une mémoire EEPROM destinée à la sauvegarde par programme de données à la coupure de l'alimentation
- Un processeur 8 bits ou 16 bits
- Faible consommation électrique

5.3 Les avantages des microcontrôleurs :

Les points forts des microcontrôleurs sont nombreux et bien réels. Il suffit, pour s'en persuader, d'examiner la spectaculaire évolution de l'offre des fabricants de circuits intègre en ce domaine depuis quelque année.

Tout a d'abord, un microcontrôleur intègre dans un seul et même boitier ce qui avant nécessitait une dizaine d'éléments séparé. Cette intégration a aussi comme conséquence immédiate de simplifier la trace du circuit imprime, puisqu'il n'est plus nécessaire de véhiculer des bus d'adresse et de données d'un composant à autre.

Aussi le microcontrôleur permet :

- Diminution de l'encombrement du matériel et du circuit imprimé
- Simplification du tracé du circuit imprimé (plus besoin de tracer de bus !)
- Augmentation de la fiabilité du système
- Nombre de composants diminues
- Connexions composants, supports et composant circuit imprimé diminues
- Intégration en technologie MOS, CMOS, ou HCMOS Diminution de la consommation

Le microcontrôleur contribue à réduire les coûts à plusieurs niveaux :

- Moins cher que les composants qu'il remplace
- Diminution des coûts de main d'œuvre (conception et montage)
- Environnement de programmation et de simulation évolués

5.4 Les mémoires :

Afin de stocker un programme, des données temporaires ou des données persistantes, le microcontrôleur dispose de plusieurs types de mémoires, ayant chacune des caractéristiques particulières.

5.4.1La mémoire vive (ou RAM)

Il s'agit d'un espace de stockage où va se dérouler l'exécution d'un programme. Elle doit être rapide en lecture et écriture. Elle est généralement volatile, c'est à dire qu'elle est remise à zéro lorsqu'elle n'est plus sous tension.

Ses caractéristiques la rendent chère, c'est pourquoi elle est en disponible de façon très limitée au sein d'un microcontrôleur (de quelques dizaines d'octets à plusieurs kilo-octets pour l'entrée de gamme). Cette limitation encourage particulièrement l'optimisation du code afin de l'utiliser et la nettoyer efficacement.

En utilisant un compilateur, le développeur n'a pas à s'occuper de la RAM, il doit seulement veiller à ne pas la gaspiller. En revanche, si on souhaite écrire un programme en assembleur, il devient nécessaire de se familiariser avec les instructions d'écriture et lecture en RAM, ainsi qu'avec l'adressage de ses secteurs.

5.4.2 La mémoire morte (ou ROM)

Cette mémoire est beaucoup plus lente mais permet de rester persistante même hors-tension. Un microcontrôleur va utiliser deux types de mémoire morte :

- La mémoire « programme », qui va contenir le code assembleur exécuter sur le processeur lors de la mise sous tension
- La mémoire « données », où le programme pourra stocker des données de façon persistante. Elle est souvent appelée EEPROM pour Electrically-Erasable Programmable Read-Only Memory (mémoire effaçable électriquement, programmable en lecture seule).

Les mémoires peuvent être stockées sur un même composant ; on distingue ensuite deux architectures :

- *Harvard*, qui va séparer l'accès (par les instructions) à la mémoire programme de la mémoire données, au point que les bus utilisés soient séparés. On peut ainsi transférer simultanément des instructions depuis la mémoire programme et des données vers la mémoire donnée
- *Von Neumann*, où une unité de contrôle gère les entrées et sorties vers une mémoire unifiée. Les instructions y sont donc des données manipulables comme celles-ci. (Il y a bien entendu d'autres subtilités, mais on restera sur celles-ci)

Bien que ROM signifie à l'origine « Read-Only Memory » (soit mémoire en lecture seule), il est possible d'y écrire et y réécrire, même depuis le programme lui-même. Sa taille varie beaucoup en fonction de la gamme, et peut aller de quelques centaines d'octets à plusieurs millions.

Il est possible d'utiliser également des mémoires externes, au travers des bus de communication. Celle-ci sont très lentes comparées à la ROM interne, mais permettent d'étendre la mémoire disponible pour des programmes très gourmands. Il faudra par contre gérer au niveau du logiciel l'écriture et la lecture depuis ces composants.

5. Les bus de communications :

5.1 Qu'est-ce que c'est ?

Beaucoup d'applications nécessitent de pouvoir communiquer avec d'autres périphériques ou systèmes. On peut trouver un ou plusieurs bus de communication Alors qu'est-ce qu'un bus de communication ? quel sont les principaux bus et leurs protocoles respectifs ?

Un bus est une topologie de réseau ou tous les nœuds sont liés à un seul lien, ce bus peut contenir plusieurs lignes toutes communes à chaque nœud du réseau.

Ainsi, toute donnée émise sur un bus est reçue par tous les nœuds en même temps (tant que le bus est constitué d'un lien physiquement court) [6].

5.2 Série ou parallèle :

Une communication de données peut être soit série, soit parallèle. Une communication parallèle transmet plusieurs flux de données simultanés sur de multiples canaux (fil électrique, piste de circuit imprimé, fibre optique, etc.) tandis qu'une communication série ne transmet qu'un seul flux de données sur un seul canal (ou médium de communication).

On aurait tendance à penser au premier abord qu'une liaison série serait moins performante qu'une liaison parallèle, dans la mesure où elle transmet moins de données sur chaque top d'horloge. Cependant, dans la majorité des cas, la fréquence d'horloge d'une liaison série est bien plus élevée que celle d'une liaison parallèle, et au final le taux de données transférées est donc plus élevé [7].

5.3 Les principaux bus :

I2C : Est un bus série permettant de transmettre des informations de façon asynchrone entre divers circuits connectés sur le bus. Le protocole de la liaison est du type MAITRE/ESCLAVE. Chaque circuit est reconnu par son adresse et peut être soit transmetteur soit receveur de l'information. Ces circuits peuvent être : Un ordinateur, un Microcontrôleur, un microprocesseur, une mémoire, un périphérique (clavier, écran,) etc.

Dans le protocole du bus I2C le circuit maître est celui qui demande un transfert d'information sur le bus et qui génère le signal d'horloge qui permet le transfert. Ainsi un circuit adressé est considéré comme un esclave.

Le bus I2C est un bus multi maître, cela signifie que plusieurs circuits peuvent contrôler le bus. Cette configuration du bus dépassant le cadre de notre cours nous étudieront seulement le cas de l'utilisation du bus avec un seul circuit maître.

Bus SPI : La liaison SPI (**S**erial Périphérique Interface) est un bus série utilisé pour la transmission synchrone de données entre un maître et un ou plusieurs esclaves (multipoints). La transmission a lieu en full duplex.

Le maître (très souvent un µC) génère l'horloge et initialise la transmission de données en sélectionnant l'esclave (convertisseur, registre à décalage, mémoire, …) avec qui il veut communiquer.

Chaque esclave est sélectionné par une ligne SS (Slave Select) et n'est actif que lorsqu'il est sélectionné.

Le bus SPI est composé de deux lignes de données et deux lignes de signal, toutes unidirectionnelles :

_ **MOSI** (Master Out Slave In) : Sur la ligne MOSI le maître transmet des données à l'esclave.

_ **MISO (**Master In Slave Out) : Sur la ligne MISO l'esclave transmet des données au maître.

_ **SCK** (SPI Serial ClocK) : Signal d'horloge, généré par le maitre, qui synchronise la transmission.

La fréquence de ce signal est fixée par le maître et est programmable.

_ **SS** (**S**lave **S**elect) : Ce signal placé au NL0 permet de sélectionner (adresser) individuellement un esclave. Il y a autant de lignes SS que d'esclaves sur le bus. Le nombre possible de raccordements SS du maître limitera donc le nombre d'esclaves.

USB : Un bus série universel (USB) est une interface commune qui permet la communication entre des périphériques et un contrôleur hôte tel qu'un ordinateur personnel (PC). Il connecte des périphériques tels que des appareils photo numériques, des souris…). Il ne fonctionne qu'avec une tension de 5V.

Un port USB standard est composé de quatre lignes :

- La masse GND

- La ligne D-
- La ligne D+
- Et l'alimentation VCC, à 5V

L'USB permet des communications :

- Entre pairs
- Synchrones et asynchrones
- En half-duplex

Sa mise en œuvre est plus complexe car il est nécessaire de décaler plusieurs champs afin de pouvoir communiquer : un identifiant fournisseur, identifiant produit, identifiant texte, un descripteur.

6. Les différents types de serrure de portes :

6.1 Type de pose :

Le premier élément qui différencie les serrures est le type de pose désiré. On distingue quatre grandes catégories de poses différentes. Voici leurs avantages et leurs inconvénients.

- La serrure encastrable : c'est la serrure de porte la plus répandue, elle est fixée dans l'épaisseur de la porte. C'est une serrure qui peut être multipoints. Elle est résistante et esthétique, mais peut fragiliser la porte.
- La serrure à poignée : une serrure intégrée à une poignée. C'est une solution très esthétique et bon marché, mais qui offre peu de résistance et de sécurité et peut fragiliser la porte.
- La serrure en applique : c'est une serrure extérieure à la porte. Un coffre en métal est fixé à la porte et un cache externe fixé sur le montant. Elle peut être à simple point ou multipoint de sécurité. C'est une serrure résistante et facile à poser, mais peu esthétique.
- La serrure carénée : c'est une serrure en applique renforcée et cachée par un capot. Elle est plus esthétique et plus solide, mais très chère [8].

6.2 Les différents systèmes de verrouillage :

La serrure à clé est sans aucun doute le système de verrouillage le plus connu, toute personne qui possède une clef est en mesure d'ouvrir la porte. Le verrouillage a carte Ce système peut être actionné soit par une carte à puce en RFID ou par une carte magnétique. Comme dans les hôtels ou

dans les entreprises. La serrure biométrique est la serrure de sécurité par excellence et utilise votre rétine ou vos empreintes digitales pour se déverrouiller.

6.3 Les serrures connectées :

6.3.1 Qu'est-ce que c'est ?

La serrure connectée : Elle a la particularité de s'ouvrir à distance, généralement sans contact grâce à une connexion Bluetooth ou internet. Ou en approchant tout simplement son badge [9].

6.3.2 Comment fonctionne une serrure connectée ?

Une serrure connectée s'ouvre lorsque sont connecteur détecte la proximité d'une clef électronique, Les clefs électroniques et les droits qui leurs sont associés sont définies par un administrateur à distance, qui n'est autre que le principal utilisateur.

7. Conclusion

Dans ce chapitre on a vu les concepts, les notions utiles et les technologies utilisées pour mieux comprendre le fonctionnement de notre système de surveillance et contrôle d'accès.

1.INTRODUCTION :

Dans ce chapitre, nous allons simuler notre projet de recherche afin de concrétiser la réalisation d'une serrure électronique codée à base de la carte ARDUINO UNO, après avoir validé notre montage par simulation.
Un système de contrôle d'accès RFID-GSM est utilisé pour contrôler l'accès et avertir qu'un accès a eu lieu pour garder une trace d'accès ou enregistrement de l'historique.

2.Méthodes et outils

2.1 Diagramme de définition de bloc

Le diagramme de définition de bloc (*bdd : Block Définition Diagram*) est un diagramme qui décrit la structure d'un système. Il est, avec le diagramme de bloc interne, un diagramme architectural[10].

Il décrit toutes les structures du système modélisé :

- Logiques
- Matérielles
- Fonctionnelles
- Ou la matière d'œuvre

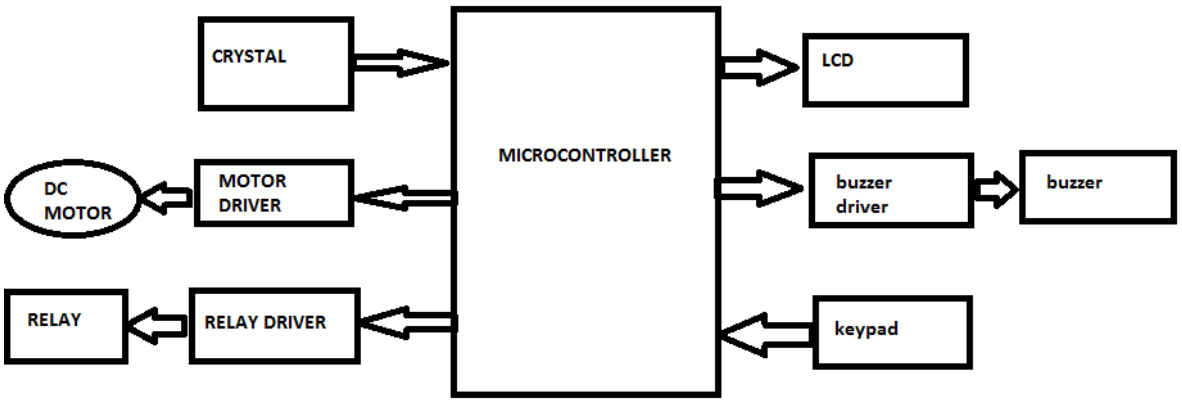

Figure14 ; Diagramme de définition de bloc de serrure codée

Ce diagramme a été implémenté en circuit. Ce schéma de circuit a été utilisé pour simuler les composants matériels du système dans Proteus 8Professional.

Dans la figure ci-dessous le schéma de circuit des composants du serrure codée :

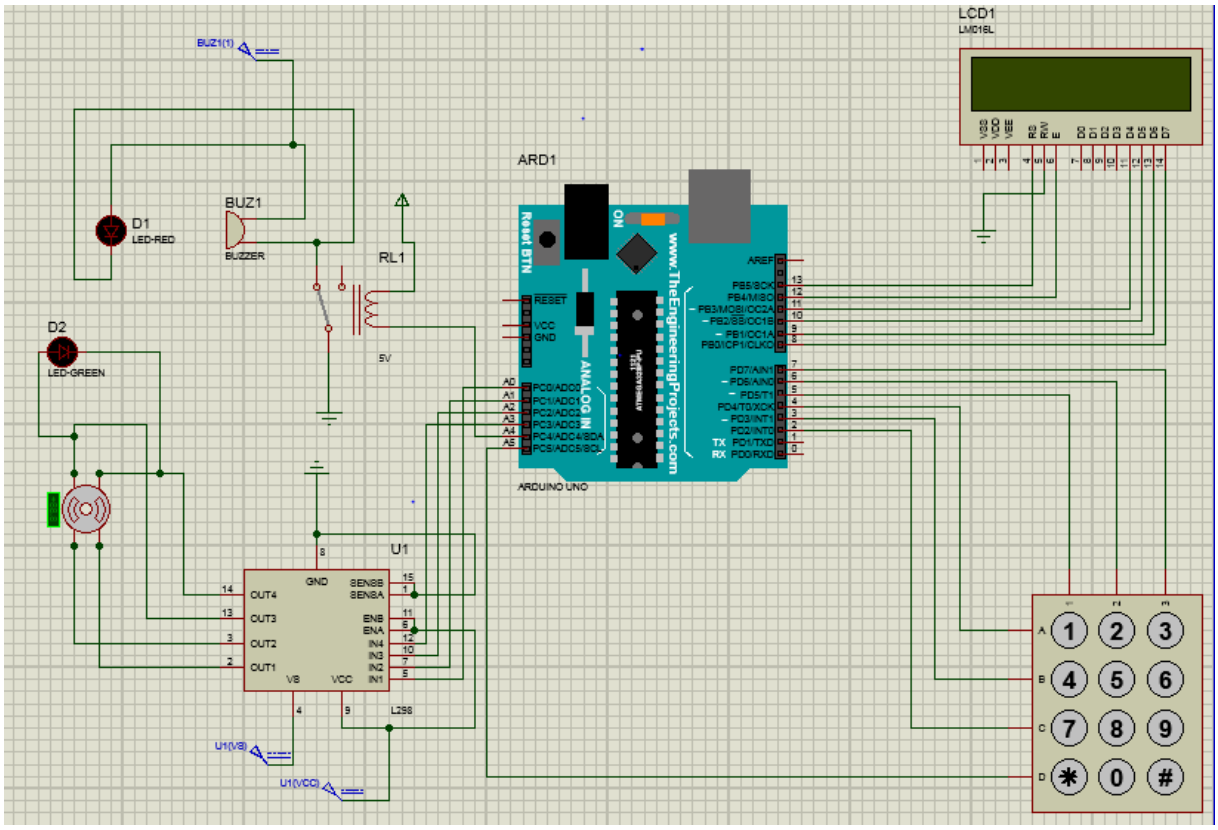

Figure15 : Schéma de serrure connecté à base Arduino

2.2 Cahier de charge

Notre cahier de charge comporte 3 étapes :

- Chaque code est composé de quatre chiffres, avec la possibilité de saisir le code jusqu'à trois tentatives différentes
- A la troisième tentative n'est pas validée, le système lance une alarme
- Donner la possibilité à l'utilisateur de modifier le code

2.3Diagramme d'activité d'un système de contrôle d'accès

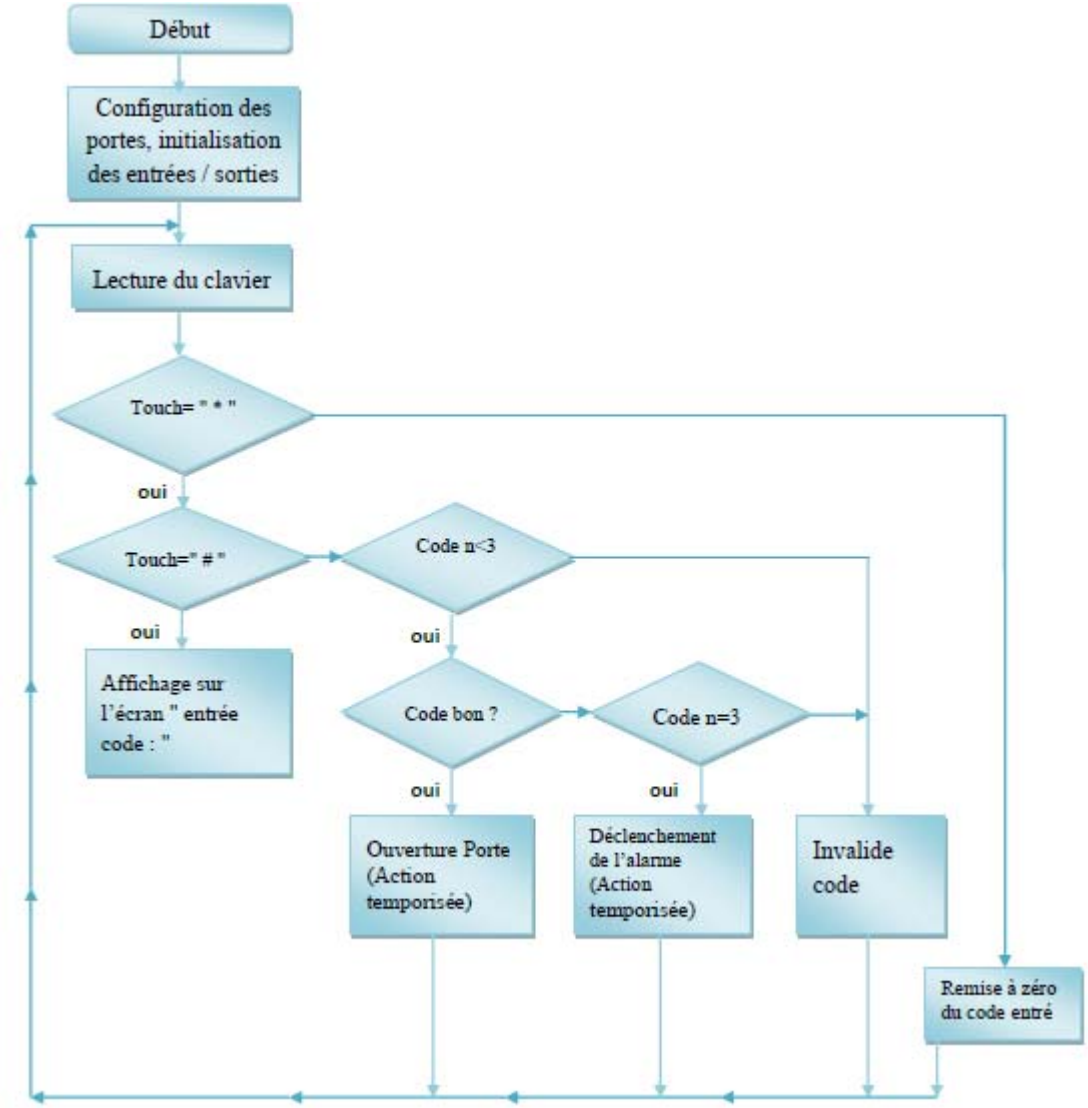

Figure 16 : Diagramme d'activité du système de contrôle d'accès

3.Simulation

3.1Simulation de la serrure codée :

Le logiciel de simulation permet de simuler des schémas électroniques ce qui permet de déceler certaines erreurs dès l'étape de conception. Indirectement, les circuits électriques conçus grâce aux logiciels de simulations peuvent être utilisé dans des documentations car le Logiciel permet de contrôler la majorité de l'aspect graphique des circuits. Et Interpréter les résultats et valider les lois physiques en électricité.

3.2Langage de logiciel de simulation :

Proteus Professional est une suite logicielle destinée à l'électronique. Développé par la société L'absenter Electronics, les logiciels incluent dans Proteus Professional permettent la CAO (Construction Assistée par Ordinateur) dans le domaine électronique. Deux logiciels principaux composent cette suite logicielle : (ISIS, ARES, PROSPICE) et VSM.

Cette suite logicielle est très connue dans le domaine de l'électronique. De nombreuses entreprises et organismes de formation (incluant lycée et université) utilisent cette suite logicielle. Outre la popularité de l'outil, **Proteus Professional** possède d'autres avantages

- Pack contenant des logiciels facile et rapide à comprendre et utiliser
- Le support technique est performant
- L'outil de création de prototype virtuel permet de réduire les coûts matériel et logiciel lors de la conception d'un projet

3.2.1 ISIS

Le logiciel « ISIS PROTEUSE » permet la création d'un schéma électronique avec une grande simplicité. Après un bref apprentissage, il est facile de développer son propre schéma électronique. L'application est accompagnée de larges librairies de composants.

Malheureusement, il y'a des composantes qui ne sont pas dans les bibliothèques fournies. Il faut donc dans un premier temps créer une librairie qui contiendra tous les composants du projet, puis créer les composants. Cette dernière tâche est réellement simplifiée puisqu'il suffit simplement de créer le contour du composant et d'ajouter ensuite les différentes broches autour de celui-ci, en prenant soin de respecter la nature de la broche (input, output, power, etc.). Ceci est capital dans la phase de vérification du schéma et de sa préparation à l'exportation vers un logiciel de routage car ce dernier pourra alors détecter d'éventuelles erreurs de connections de broches de composants (par exemple la connexion d'une sortie sur une autre sortie).

3..2.1 ARES :

Le logiciel ARES est un outil d'édition et de routage qui complète parfaitement ISIS. Un schéma électrique réalisé sur ISIS peut alors être importé facilement sur ARES pour réaliser le PCB (**Printed circuit board)** de la carte électronique. Bien que l'édition d'un circuit imprimé soit plus efficiente lorsqu'elle est réalisée manuellement, ce logiciel permet de placer automatiquement les composants et de réaliser le routage automatiquement.

C’est un logiciel de programmation par code, ce dernier contient une cinquantaine de commandes différentes. A l’ouverture, l’interface du logiciel ressemble à ceci Le développement sur Arduino est très simple :

- On code l'application : Le langage Arduino est basé sur les langages C/C++, avec des fonctions et des librairies spécifiques à Arduino (gestions des E/S),
- On relie la carte Arduino au PC et on transfert le programme sur la carte,
- On peut utiliser le circuit.

Le logiciel de programmation des modules Arduino est une application Java multiplateformes (fonctionnant sur tout système d'exploitation), servant d'éditeur le code et le compilateur, et qui peut transférer le firmware (et le programme) au travers de la liaison Série (RS232, Bluetooth ou USB selon le module) [11].

3.3 Mise en œuvre de l’environnement Arduino

- On conçoit d’abord un programme avec le logiciel Arduino (voir Annexe 05)
- On vérifie ce programme avec le logiciel (compilation)
- Des messages d’erreur apparaissent éventuellement...on corrige puis vérifie à Nouveau...
- On enlève le précédent programme sur la carte Arduino (Bouton réinitialisation)
- On envoie ce programme sur la carte Arduino dans les 5 secondes qui suivent

L’initialisation ;

- L’exécution du programme sur la carte est automatique quelques secondes plus tard ou à ses prochains branchements sur une alimentation électrique (Alim 9/12V ou port USB.

3.4 Résultat da la simulation

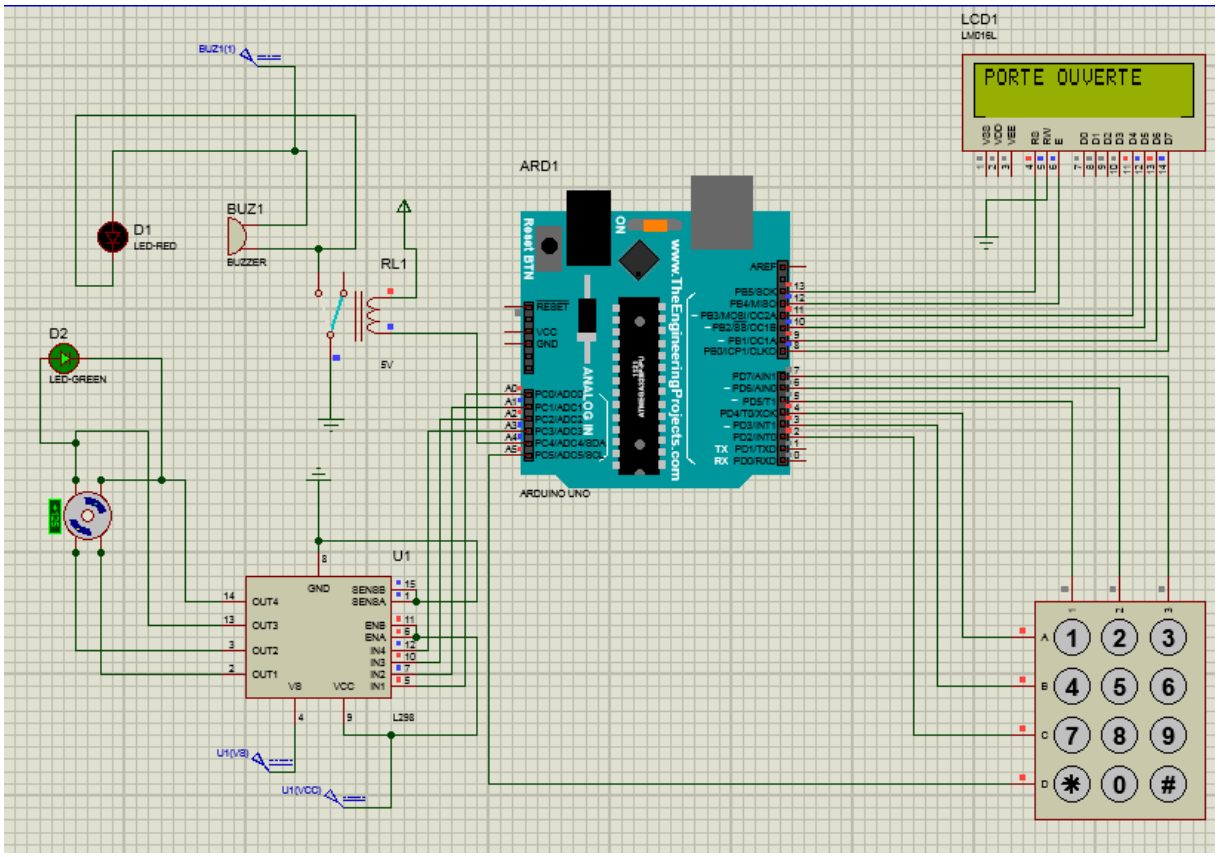

Figure17 : Schéma de serrure électronique a base ARDUINO UNO après simulation

- L'Arduino UNO alimenté le driver moteur L298, ce dernier commande le moteur pas à Pas qui nous permet l'ouverture de porte.
- Le Buzzer BUZ1 sert à tester le fonctionnement de l'alarme,
- La LED D1 s'allume lorsque le code saisi est erroné,
- La LED D2 s'allume lorsque le code saisi est correct,
- Le pavé numérique c'est là où l'utilisateur saisi le code,
- L'afficheur LCD1 permet l'interaction entre l'utilisateur et le système.

4.Système de contrôle d'accès RFID-GSM

4.1 Présentation :

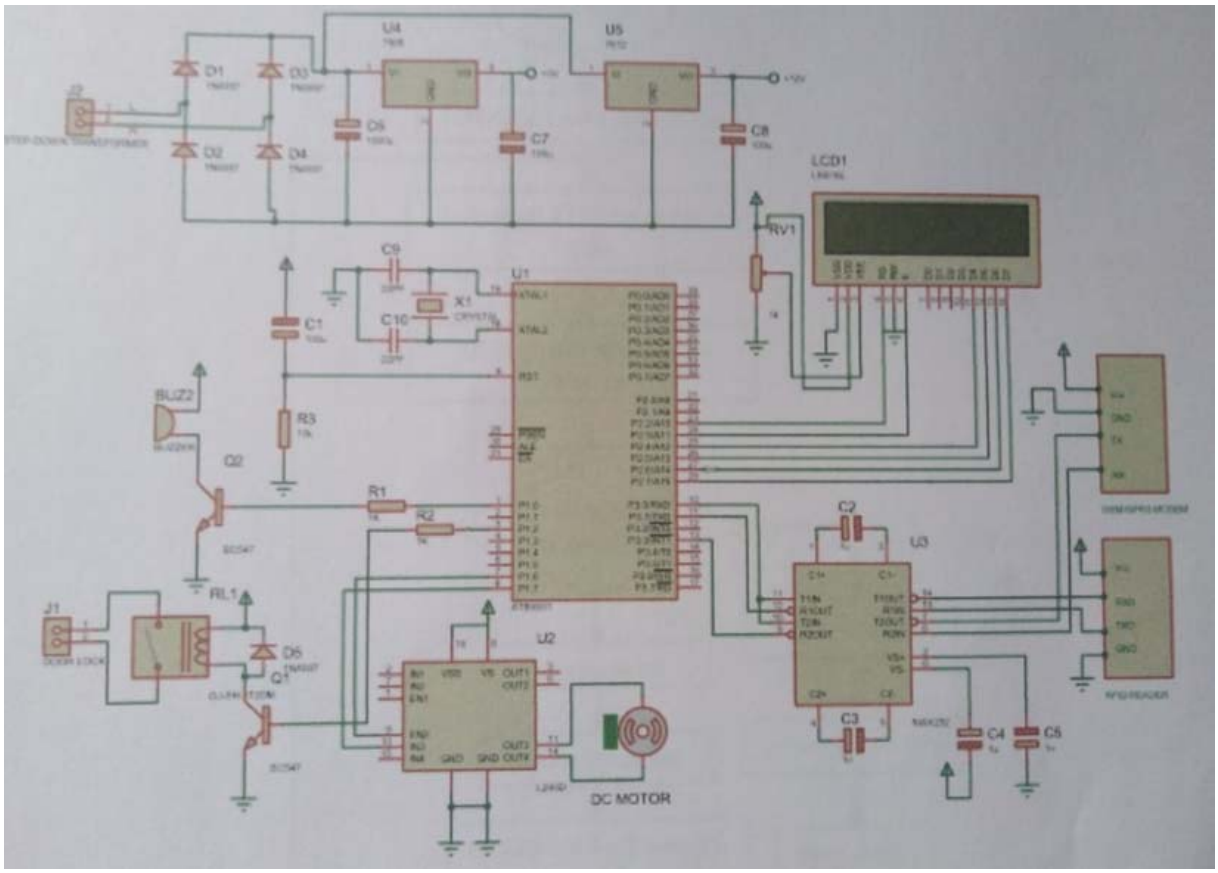

Figure18 : Le circuit global du système de contrôle d'accès RFID-GSM

Le système est basé sur l'identification par radio fréquence 125KHz. Le microcontrôleur envoie des signaux de contrôle (moteur DC, buzzer, un afficheur LCD, un modem GSM/GPRS, relais).

Les tags RFID autorisés sont stockés dans le microcontrôleur, lorsque l'utilisateur présente son tag devant le lecteur les informations uniques de celui sont comparées avec celles contenus dans le microcontrôleur et dès qu'il y a une correspondance, le microcontrôleur allume le moteur DC via un driver L293D, le numéro de l'utilisateur et son identificateur de carte s'affichent sur l'écran LCD, le BUZZER s'allume pendant 5 secondes avec l'activation de GSM/GPRS pour envoyer un SMS d'avertissement.

4.2Méthodes et outils

4.2.1 Le diagramme de définition de bloc :

Circuit globale du système de contrôle d'accès RFID-GSM

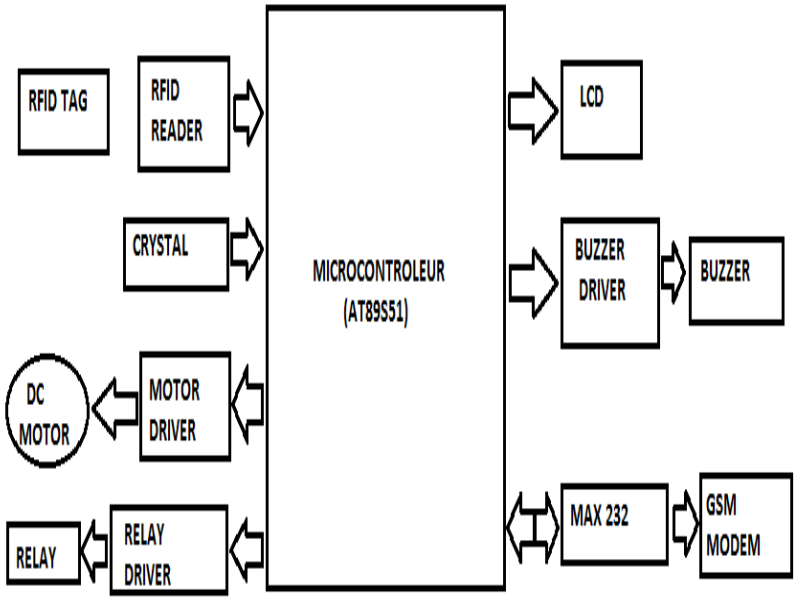

Figure19 : Diagramme de définition de bloc du système de contrôle d'accès RFID-GSM

4.3 Système du suivi de la présence

4.3.1 Présentation :

Ce système a été principalement conçu pour suivre la présence des étudiants. Il est basé sur l'utilisation de la technologie RFIDL. Chaque étudiant lui offre l'option de participation dans le système, s'il refuse ou il oublie son tag RFID, l'option de signer sur une feuille de présence est lui proposée également.

Au début du semestre, chaque étudiant choisi son propre tag RFID. L'instructeur alors enregistre chaque identificateur du tag RFID dans le lecteur, ensuite le lecteur émit l'identificateur à la base de données là ou il est enregistré avec la date et le temps précis. Ces données ont été enregistré sous format texte ce qui facilite l'exportation vers tout logiciel de traitement. Une fois tout est paramétrer, les données pourrait être triées par id, nom, temps.

La surveillance a été effectuée en utilisant le logiciel EXEL.

4.3.2 Méthode et outils :

Le système du suivi de la présence repose sur l'utilisation d'un lecteur RFID opère sur la fréquence 125KHz muni d'un port USB ce qui lui donne la flexibilité d'être connecté à n'importe quel ordinateur, les tags RFID utilisé opèrent sur la même fréquence et ils sont portables qu'on pourrait facilement les mettre dans un porte-clés.

Le système à 125KHz a été choisi parce qu'il s'agit d'une basse fréquence. Cela signifie que les étudiants doivent approcher du podium, ou le scanner est situé, pour marquer leur présence.

De cette façon, il est plus visible pour le professeur si un étudiant essaie de marquer ses collègues, de plus, le fait qu'il base sur une fréquence de 125KHz cela signifie que les élèves ne doivent pas s'inquiéter que tous leurs mouvements sont suivis à travers le campus.

Le système de présence suggéré est basé sur un ensemble de Marcos Excel, le lecteur RFID lit les tags RFID comme des chiffres en entrée par conséquence, chaque fois que le tag est à proximité du lecteur RFID,10 chiffres sont envoyés à l'ordinateur. Cela signifie que les formateurs peuvent prendre les identificateurs RFID sur un simple éditeur de texte, tel que bloc-notes, Windows. Cependant, il n'y aurait pas de date ou l'heure. Les macros Excel fournies sont un moyen simple de lire les tags via le lecteur RFID et de fournir une date et l'heure pour chaque entrée de présence. Les macros Excel sont fournies à titre indicatif et les instructeurs peuvent écrire leur code en utilisant n'importe quel langage de programmation.

Lorsque l'instructeur ouvre le fichier EXCEL, il voit quelque chose comme la figure ci-dessous, mais sans aucun nom ou numéro RFID dans la feuille de travail « Etudiants ». L'instructeur doit ensuite inscrire chaque étudiant à un numéro RFID. Il suffit d'entrer le nom de l'étudiant dans la colonne A, et le numéro d'identification dans la colonne B, plutôt que de taper le nombre, puis scannez l'étiquette RFID. La numérisation est accomplie en plaçant l'étiquette RRFID à 10 chiffres dans la cellule. L'enregistrement prend environ 10-20 secondes par étudiant. Si, au cours du semestre, un étudiant perd ou casse son étiquette RFID, l'instructeur peut simplement remplacez l'ancien numéro par le nouveau dans la feuille de travail « Etudiants ».

5. Conclusion

Ce chapitre a été consacré à la présentation des systèmes étudiés, d'où l'utilité de traiter notre système de surveillance et contrôle d'accès.

1.Introduction

Dans ce chapitre nous allons nous concentrer sur la définition de l’architecture du système ainsi que sur l’analyse et la conception des besoins et des exigences des utilisateurs qui permet de traduire les besoins fonctionnels et de la spécification des exigences dans un langage plus professionnel et compréhensible par tous les individus intervenants dans la réalisation et l’utilisation de l’application.

2 Conception de l’application embarquée

2.1 Diagramme de cas d’utilisation :

Un diagramme de cas d'utilisation capture le comportement d'un système, d'un sous-système, d'une classe ou d'un composant tel qu'un utilisateur extérieur le voit. Il scinde la fonctionnalité du système en unités cohérentes, les cas d'utilisation, ayant un sens pour les acteurs. Les cas d'utilisation permettent d'exprimer le besoin des utilisateurs d'un système, ils sont donc une vision orientée utilisateur de ce besoin au contraire d'une vision informatique [13].

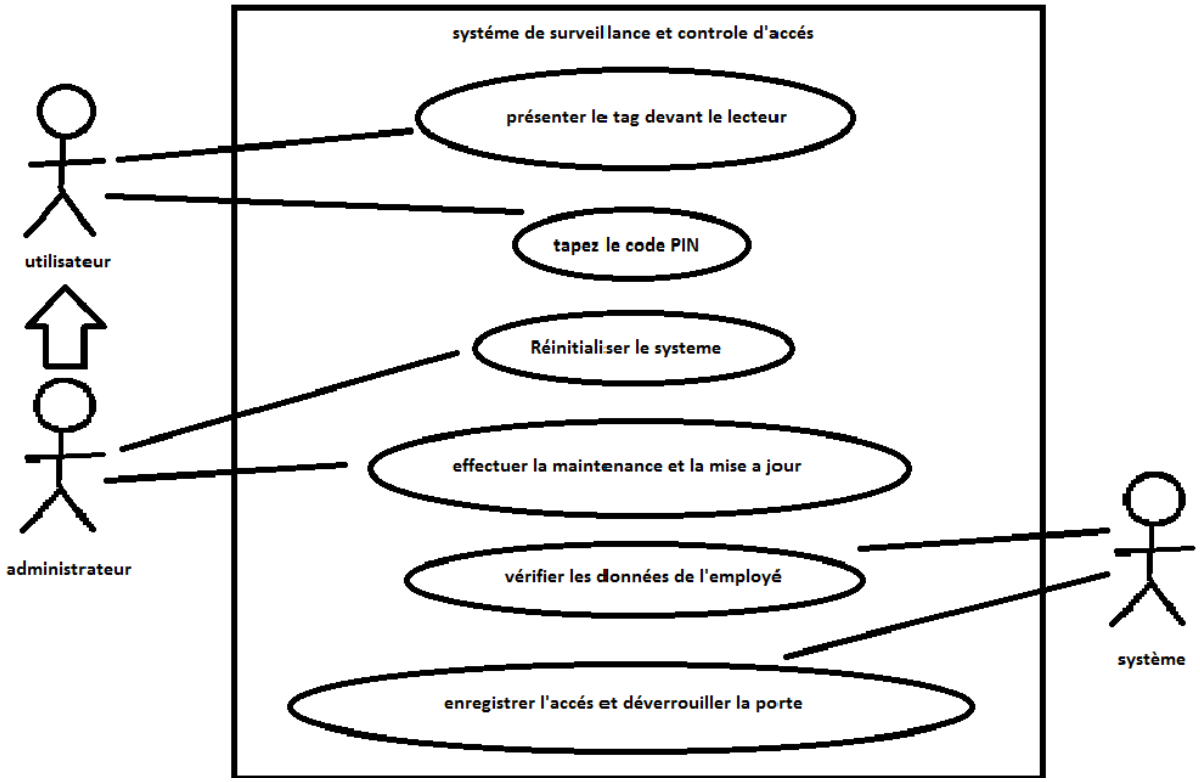

Figure20 : Diagramme des cas d’utilisation de système de surveillance et contrôle d’accès

2.2 Description textuelle

2.2.1 Le cas « présenter le badge devant le lecteur » :

Nom : présenter le badge devant le lecteur.

Objectif : la reconnaissance du badge par le système et le déclenchement du cas d'utilisation « taper code PIN ».

Acteurs principaux : l'employé, administrateur.

Acteurs secondaires : le système.

Préconditions :

- Le système doit être fonctionnel.
- Le message « scan badge » affiché sur l'écran.
- L'employé possède un badge RFID.

Scénario nominal :

- Employé présente le tag devant le lecteur.
- Système affiche « tapez code PIN ».

Scénario alternatif :

- Badge non valide.
- Système affiche « accès refusé ».

Post-conditions : le système demande de l'employé de valider son entrée par un code PIN.

2.2.2 Le cas « tapez code PIN » :

Nom : taper code PIN.

Objectif : confirmer le badge scanné et le système déverrouille la porte.

Acteurs principaux : l'employé, administrateur.

Acteurs secondaires : le système.

Précondition :

- Présentation d'un badge valide.

- Le message « tapez code PIN » affiché sur l'écran.
- Taper code PIN.

Scénario nominal :

- L'employé tape son code PIN.
- Système affiche « porte ouverte » et déverrouille la porte.

Scénario alternatif :

- Code PIN erroné.
- Système fournie trois fois d'essais, si on dépasse trois essais le système réinitialise.

Post-conditions : le système déverrouille la porte et l'employé pourrait entrer.

2.3 Diagramme d'activités

Un diagramme d'activité permet de modéliser le comportement du système, dont la séquence des actions et leurs conditions d'exécution. Les actions sont les unités de base du comportement du système.

Un diagramme d'activités permet de grouper et de dissocier des actions. Si une action peut être divisée en plusieurs actions en séquence, vous pouvez créer une activité les représentant [14].

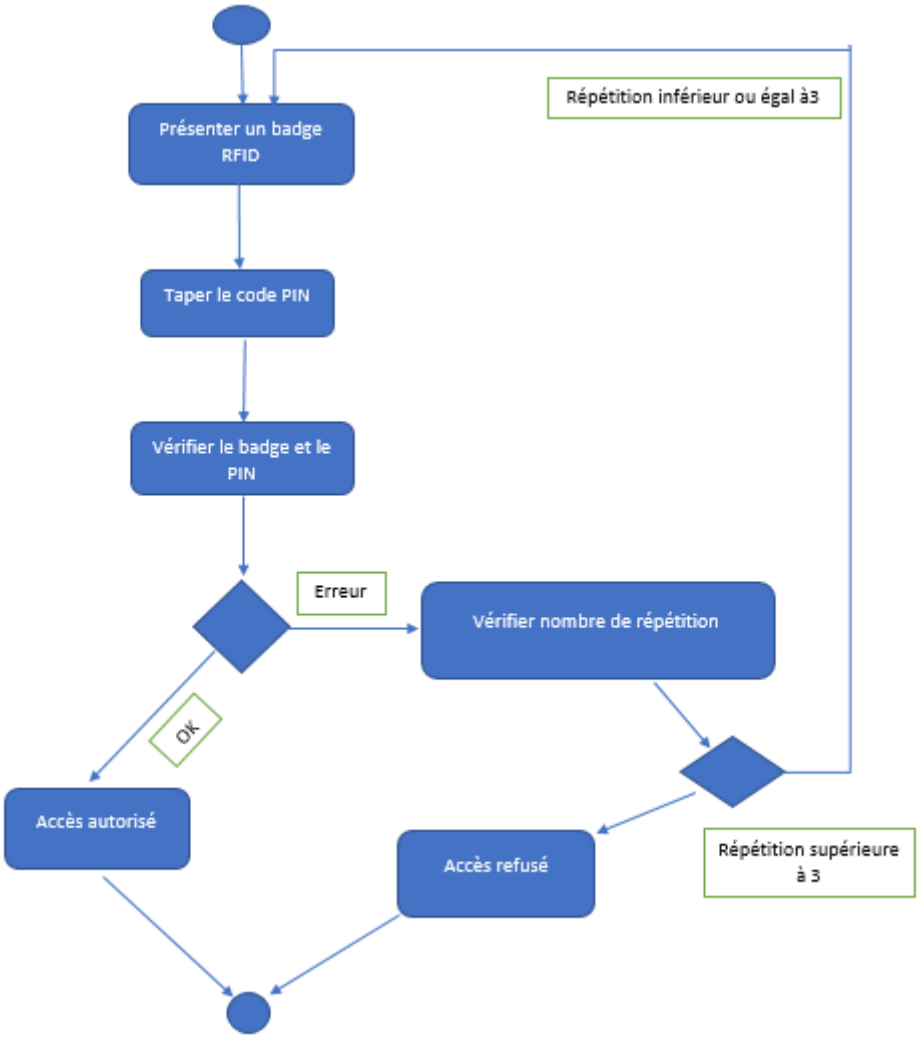

Figure21 : Diagramme d'activité du système de surveillance et contrôle d'accès

2.4 Diagramme de séquence

Les diagrammes de séquences sont la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique dans la formulation Unified Modeling Language [15] .

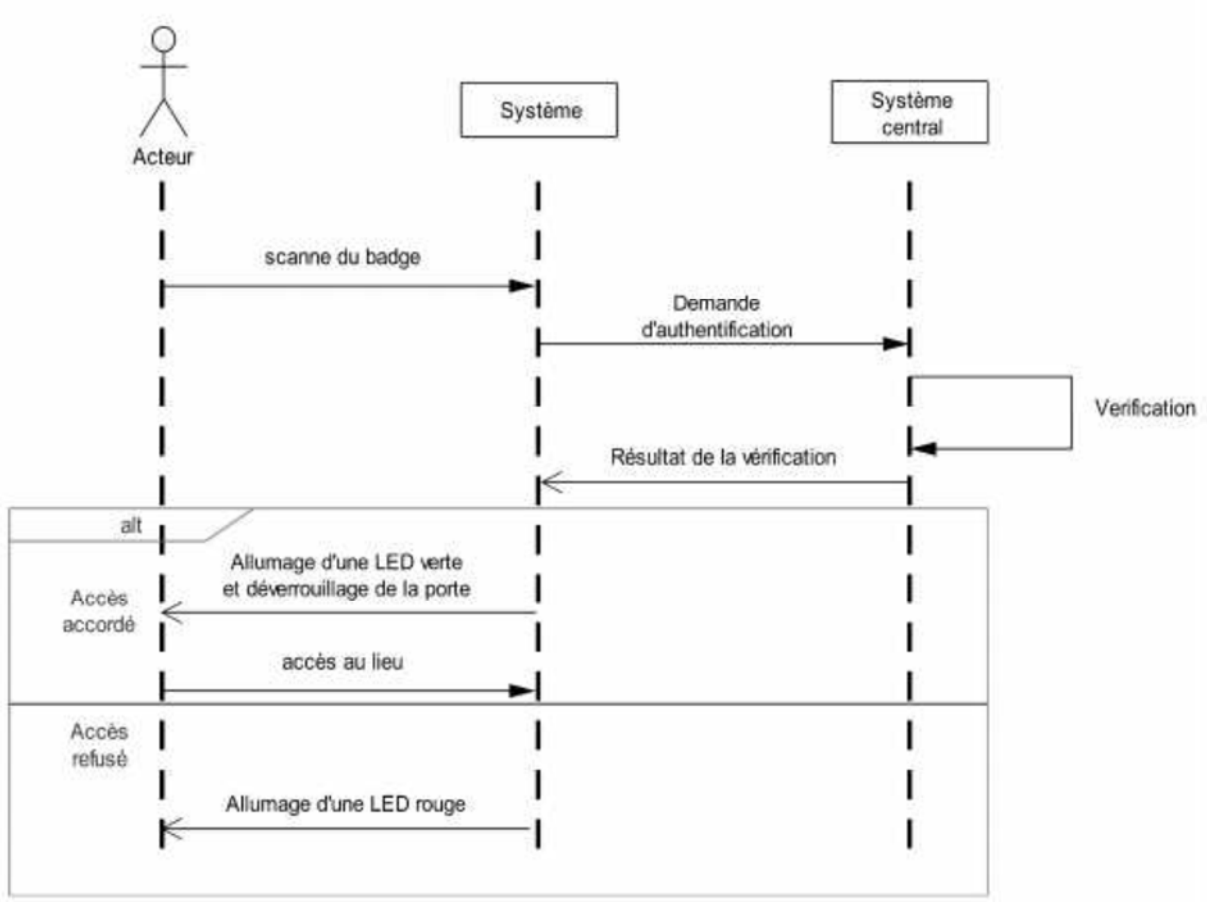

Figure22 : Diagramme de séquence du système de surveillance et contrôle d'accès

3. Conception de la plateforme de surveillance

Nous utilisons une application web qui sert comme plateforme de notre système de surveillance et contrôle d'accès, l'administrateur pourrait faire la gestion des utilisateurs en effectuant des opérations standards.

3.1 Diagramme de cas d'utilisation

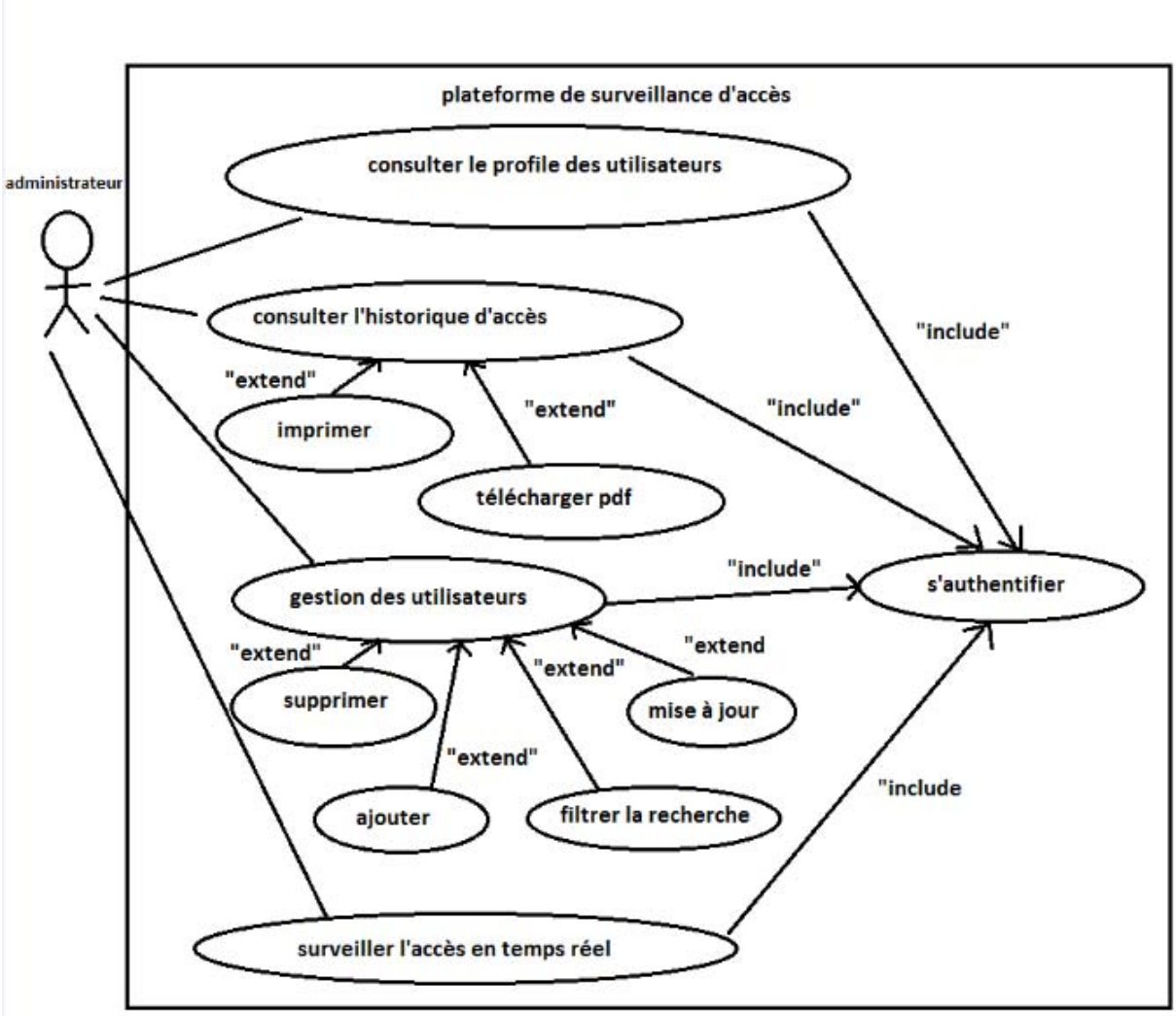

Figure23 : Diagramme de cas d'utilisation de la plateforme d'accès

3.2 Description textuelle

3.2.1 Le cas « consulter l'historique d'accès » :

Nom : consulter l'historique d'accès.

Objectif : avoir accès aux historiques d'accès des utilisateurs.

Acteurs principaux : administrateur.

Acteurs secondaires : il n'y a pas.

- **Préconditions :**

Scénario nominale :

- L'administrateur tape son nom d'utilisateur et son mot de passe.
- Accès à la plateforme de surveillance d'accès.

Post-conditions : consulter l'historique d'accès et de pouvoir l'imprimer ou le télécharger.

3.2.2Le cas « gestion des utilisateurs » :

Nom : gestion des utilisateurs.

Objectif : avoir accès à la plateforme de surveillance d'accès.

Acteurs principaux : administrateur.

Acteurs secondaires : il n'y a pas.

Précondition :

- S'authentifier.

Scénario nominale :

- L'administrateur tape son nom d'utilisateur et son mot de passe.
- Accès à la plateforme de surveillance d'accès.
- Effectuer l'opération voulue.

Post-conditions : effectuer la gestion des utilisateurs.

3.3 Diagramme d'activité

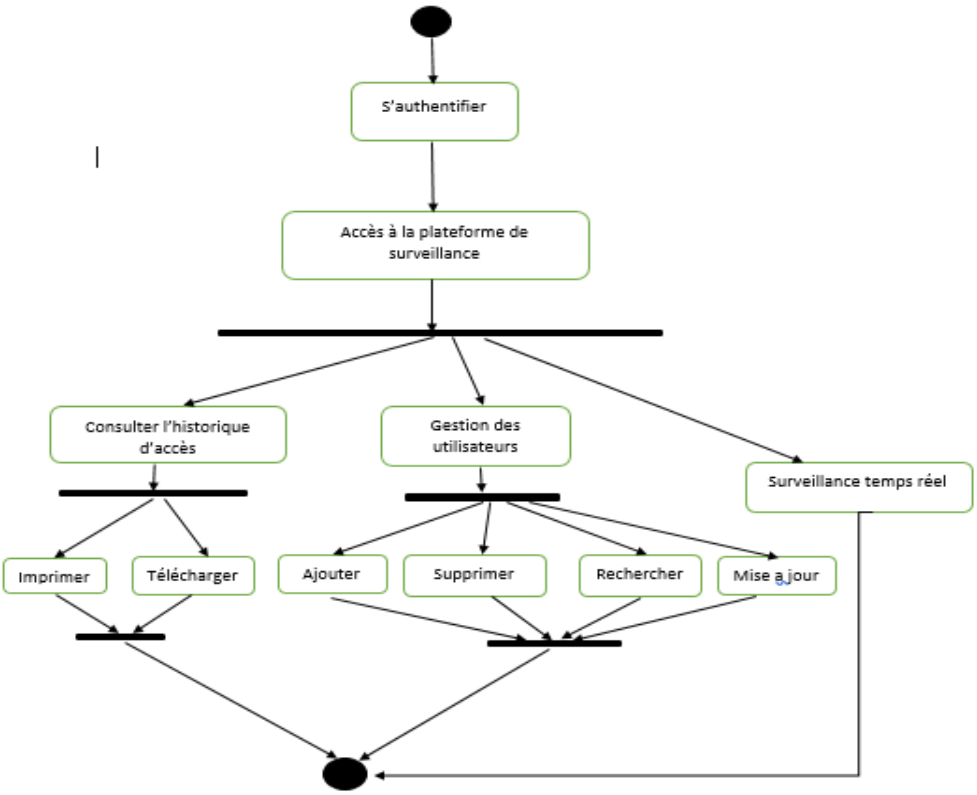

Figure24 : Diagramme d'activité de la plateforme de surveillance d'accès

3.4 Diagramme de classes

Il représente les classes intervenant dans le système. Le diagramme de classe est une représentation statique des éléments qui composent un système et de leurs relations.

Chaque application qui va mettre en œuvre le système sera une instance des différentes classes qui le compose.

A ce titre il faudra bien garder à l'esprit qu'une classe est un modèle et l'objet sa réalisation[16].

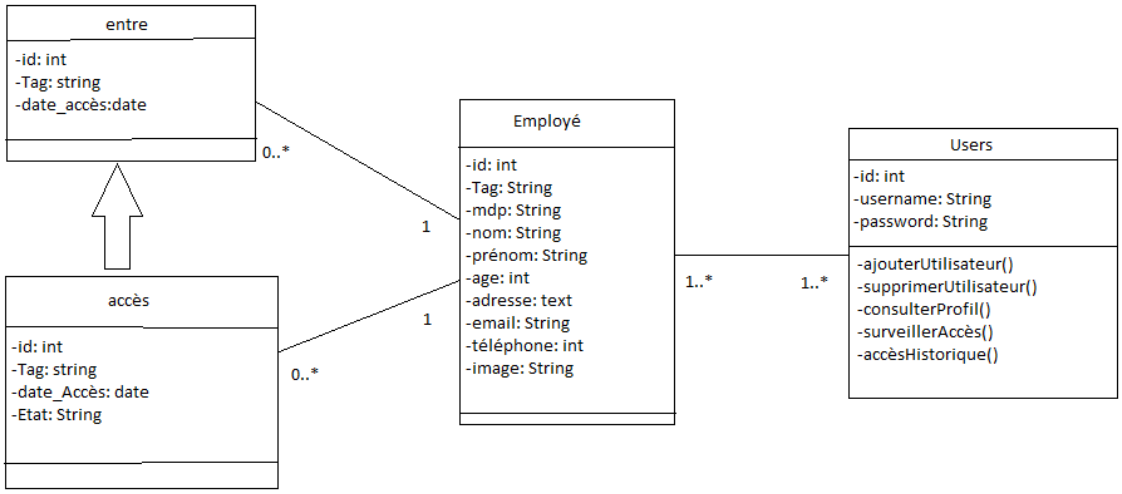

Figure25 : Diagramme de classe de la plateforme de surveillance d'accès

4.Conclusion ;

Dans ce chapitre toutes les questions concernant la manière de réaliser le système à développer ont été expliquées. Le produit obtenu est un modèle graphique prêt à être codé.

1.Introduction :

Dans ce chapitre on va commencer la partie réalisation et implémentation de notre système de surveillance d'accès. Pour réaliser notre système d'accès on a besoin de :

- Connecter le module RFID au microcontrôleur
- Connecter la serrure électrique au microcontrôleur
- Connecter notre écran OLED au microcontrôleur
- Connecter le microcontrôleur avec le serveur
- Création d'une application web qui sert comme plateforme de surveillance de tout le système.

2.Hardware

2.1 Module RFID MFRC522 :

Le module RC522 est une interface qui permet l'identification sans contact à partir d'un badge ou une clé RFID. Lancé par la société NXP, Il est basé sur le circuit intégré Philip RC522, il communique avec Arduino via l'interface SPI. Il utilise la bande ISM 13.56MHz, la distance de communication peut aller jusqu'à 6cm mais la plupart des modules NFC marchent très bien avec 1cm de distance, il s'agit d'une puce sans contact à basse tension, à faible cout et de petite taille, un choix idéal pour les instruments intelligents et portables.

Le mécanisme RFID/NFC se base sur une radio communication de courte distance, ils utilisent la norme ECM-A340 et ISO/IEC 18092. Le MFRC522 utilise un concept avancé de modulation et de démodulation qui est entièrement présenté dans tous les types de protocoles et de méthodes de communication sans contact à 13,56 MHz, il prend en charge l'algorithme de cryptage CRYPTO1 pour vérifier les produits MIFARE de communications sans contact à haute vitesse, avec un débit de transmission de données bidirectionnel pouvant atteindre 424 kbits/ S. En tant que nouveau produit de la série de cartes de lecteur hautement intégrées de 13,56 MHz, il communique avec la machine hôte via le mode série, vous pouvez choisir entre I2C, SPI, UART en série. Ce module est idéal pour des projets de domotique pour identifier la personne avec son badge avant d'ouvrir la porte. Il peut être utilisé dans n'importe quel projet d'identification.[17].

Figure26 : Module RFID MFRC522

2.1.1 Caractéristiques :

- Basée sur la puce Philips MFRC522
- Power Voltage : 3.3V
- Current :13-26mA
- Fréquence d'utilisation : 13.56MHz
- Distance opérationnelle : 0 ~ 60mm
- Interface : SPI
- Dimensions : 40mm × 60mm
- Module Name : MF522-ED
- Working current：13—26mA/ DC 3.3V
- Standby current：10-13mA/DC 3.3V
- Sleeping current：<80uA
- Peak current：<30mA
- data communication speed：Maximum 10Mbit/s
- Card types supported：mifare1 S50、mifare1 S70、mifare UltraLight mifare Pro、mifare Desfire
- Working temperature：-20—80 degree

- Storage temperature : -40—85 degree
- Humidity : relevant humidity 5%—95%
- Max SPI speed : 10Mbit/s

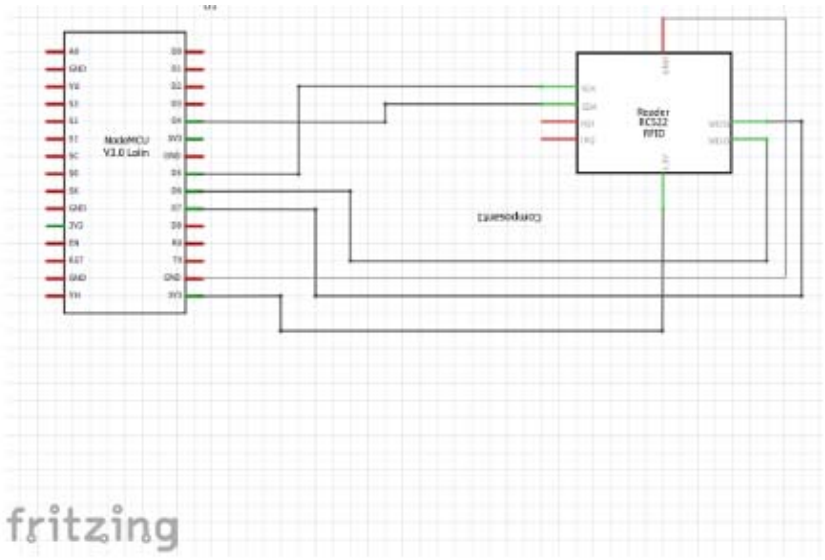

Figure27 : Circuit microcontrôleur avec MFRC522

2.2 Le microcontrôleur NodeMCU Lolin V3 :

Ce composant embarque un module Wifi, de la mémoire, une liaison série et gère des ports GPIO. Tout cela en quantité différente en fonction de la version.

NodeMCU est une plate-forme open source IoT, matérielle et logicielle, basée sur un SoC Wifi ESP8266 ESP-12 fabriqué par Espressif Systems. Le terme « NodeMCU » se réfère par défaut au firmware plutôt qu'aux kits de développement. Le firmware, permettant nativement l'exécution de scripts écrits en Lua, est basé sur le projet eLua et construit sur le SDK Espressif Non-OS pour ESP82668. Il utilise de nombreux projets open source comme lua-cjson9 et spiffs [18].

Figure28 : Le module NodeMCU

2.2.1 Alimentation électrique :

La tension de fonctionnement de l'ESP8266 est de 3.3v.

Il faudra donc être vigilent au niveau des GPIO à ce que les composants connectés respectent cette tension.

Il existe plusieurs possibilités pour alimenter électriquement le NodeMCU comme on peut le voir sur la page « http://henrysbench.capnfatz.com/henrys-bench/arduino-projects-tips-and-more/powering-the-esp-12e-nodemcu-development-board/ »

Le schéma ci-dessous, qui en est extrait, montre les pins sur lesquels on peut raccorder une alimentation électrique ainsi que la tension maximum pour chacun.

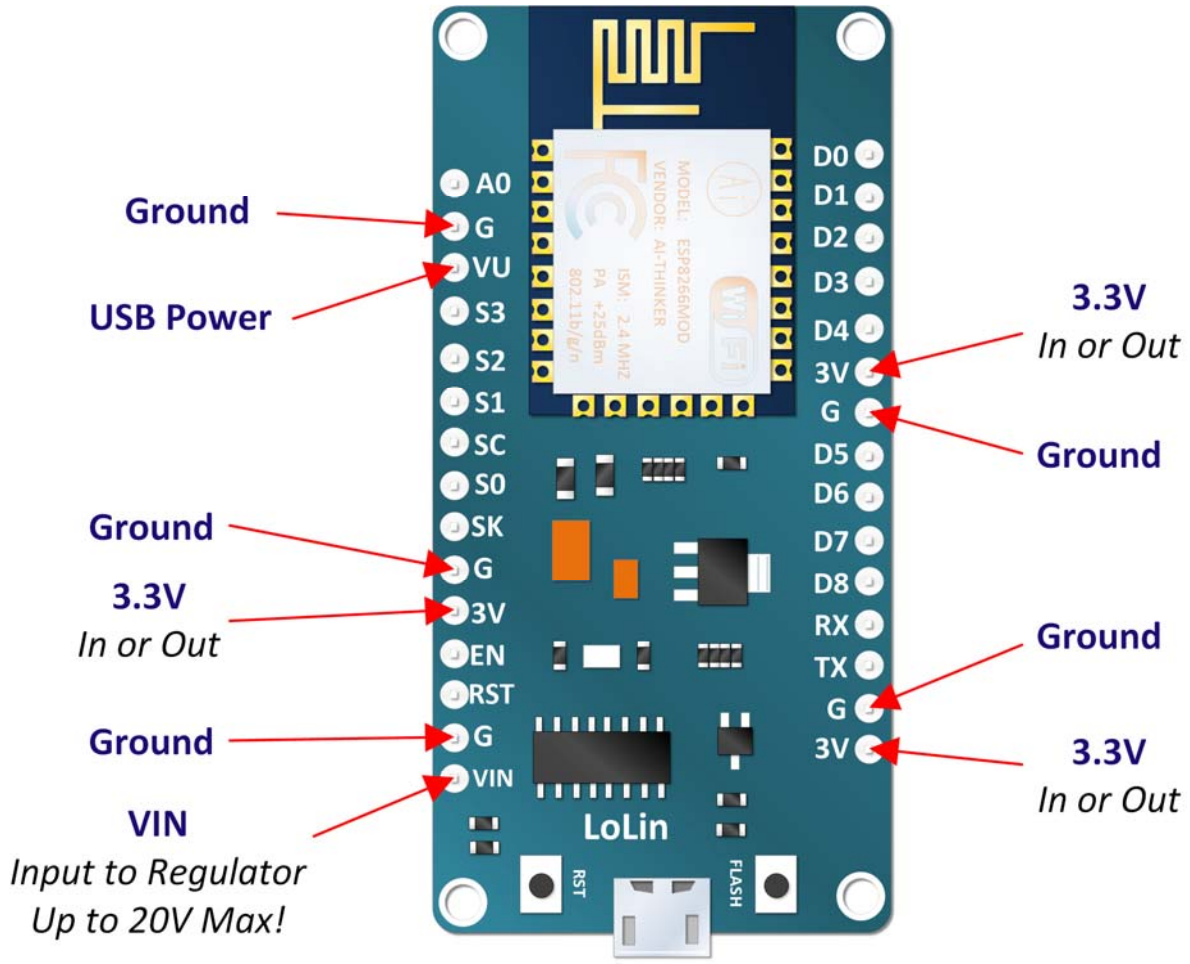

Figure29 : Les pins d'alimentation du NodeMCU

Attention toutefois à ce qui est indiqué pour l'alimentation sur VIN ! Dans de nombreux documents j'ai vu que cette tension doit être comprise entre 3.3V et 9V maximum. Contrairement à ce qu'il y a d'indiqué sur l'image ci-dessus, il ne faudra en aucun cas dépasser cette tension d'entrée (9V donc !).

On voit donc que la carte s'alimente en connectant une source électrique 3.3V sur une des bornes 3.3V, en se connectant en micro USB avec câble USB ou en connectant une source sur VIN.

2.2.2 Mémoire :

Les ESP8266 embarquent une plus ou moins grosse mémoire flash accessible en SPI. Cette mémoire peut être intégrée au processeur ou alors associée sur la carte NodeMCU comme mémoire flash externe.

Ce qui est intéressant à connaitre, c'est que la mémoire flash est structurée de la manière suivante :

- Un espace de stockage pour le firmware
- Un espace de stockage temporaire pour les mises à jour OTA (Over The Air) du firmware
- Un système de fichier SPIFFS
- Un emplacement EEPROM pour la sauvegarde de données par les programmes
- Un emplacement pour stocker la configuration du WIFI dans le cas de l'utilisation du SDK natif

Dans la carte NodeMCU v3 il y a 4M de mémoire, dont 3 peuvent être dédiés au système de fichier. Ce système de fichier peut être utilisé pour y stocker des données et des fichiers, pour un serveur web par exemple. Cependant n'y voyez pas l'équivalent d'une file system moderne. Il n'y a pas de correction d'erreur et il n'y a pas d'arborescence de fichier (répertoires et sous répertoires), tout est au même niveau. Mais comme le caractère / est accepté dans un nom de fichier, vous pouvez stocker un fichier du nom de "/web/index.htm" si vous voulez avoir quelque chose de structuré. Attention cependant les noms de fichiers sont limités à 32 caractères, y compris le '\0' de fin de chaine (donc 31 caractères utiles).

La mémoire EEPROM est particulièrement intéressante car c'est dans cette dernière que pourront être sauvegardées de données persistantes pour nos programmes. Par exemple, si une variable de notre programme sert à mémoriser un mot de passe et que ce mot de passe peut être changer, s'il est stocké dans la mémoire EEPROM nous pourrons retrouver ce changement en cas de reboot ou de coupure électrique.

2.2.3 Programmation de NodeMCU :

L'ESP8266 peut se programmer de plusieurs façons :

Avec des scripts Lua interprétés ou compilés, avec le firmware NodeMCU

- En C++, avec l'IDE Arduino
- En JavaScript, avec le firmware Espruino
- En MicroPython, avec le firmware MicroPython
- En C, avec le SDK d'Espressif ou avec le SDK esp-open-sdk3

Pour ma part j'ai utilisé une carte NodeMCU, connectée en USB à mon PC et programmée avec l'IDE Arduino.

2.2.4 Bon à savoir pour programmer la bête :

Lorsque le programme est compilé, il faut l'injecter dans le microcontrôleur. On appelle cela flasher le composant car notre programme deviendra le firmware de ce dernier.

Normalement, la carte NodeMCU se met automatiquement en mode apprentissage et normalement il n'y a rien à faire avant de télé verser le programme depuis l'IDE Arduino. Dans la pratique ceci ne fonctionne pas toujours. Je n'ai pas encore bien identifié les conditions préalables pour que ce mode "flash" soit toujours opérationnel automatiquement. J'ai pu constater que cela dépend de ce qui est connecté aux PINs et aussi si c'est la première fois que le composant est flashé.

Quand le « flashage » de la carte échoue, il faut remettre la carte dans le mode apprentissage en utilisant les boutons situés de part et d'autre du port micro USB comme indiqué ci-dessous :

- Appuyez sur le bouton Flash et maintenez le bouton appuyé.
- Appuyez sur Reset
- Relâchez le bouton Reset
- Relâchez le bouton Flash

Ceci est valable pour les cartes NodeMcu. Pour les autres modèles, par exemple ESP-01, on accède au mode "flash" en connectant certaines PINs aux pôles V+ ou GND.

2.2.5 Définition des pins :

En ce qui concerne les cartes NodeMCU :

Il existe plusieurs constructeurs qui proposent des cartes Nodemcu (LoLin, Amica, …). On trouve aussi des cartes sans marques.

Il existe également plusieurs versions de la carte. On trouve souvent sur le net des références aux versions 0.9, 1.0, 2.0 et 3.0 (décembre 2017).

En fonction de la version de la carte, l'architecture des PIN GPIO peut varier. Mais ces variations sont souvent minimes.

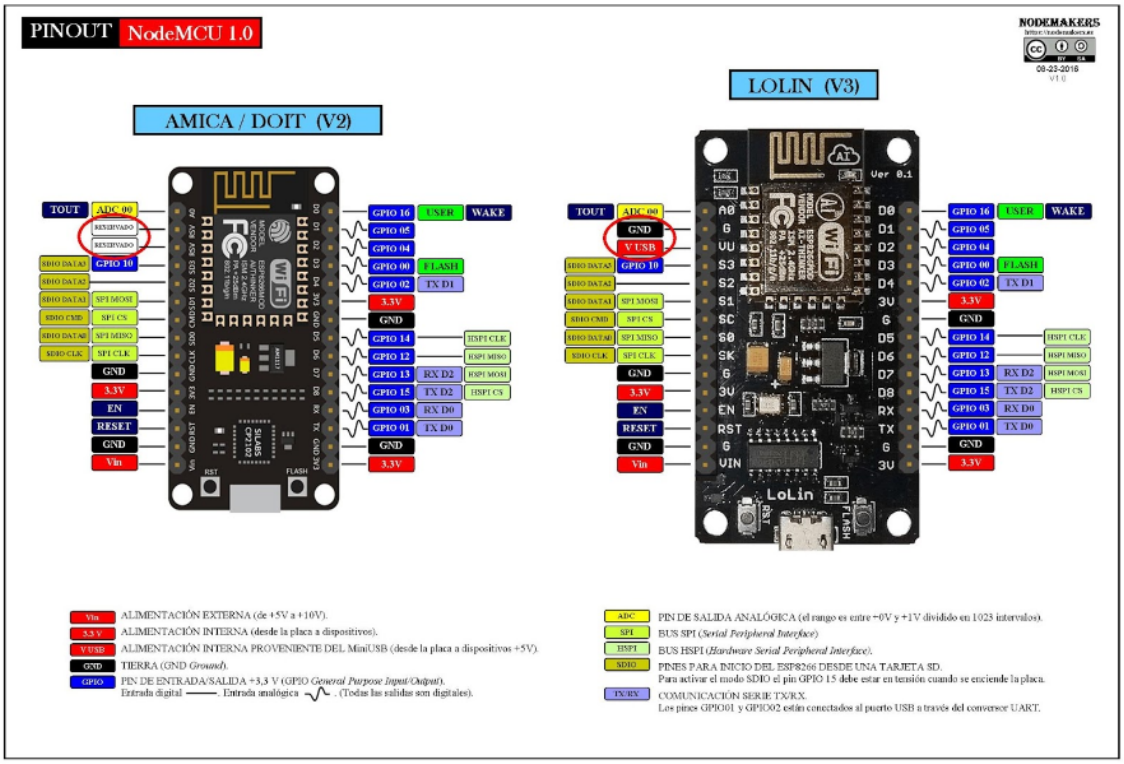

Figure30 : Définition des pins du NodeMCU

3.L'écran OLED :

Ces écrans sont petits, seulement environ 1" de diagonale, mais très lisibles en raison du contraste élevé d'un écran OLED. Cet écran est composé de 128x32 pixels OLED blancs individuels, chacun étant allumé ou éteint par la puce du contrôleur. Comme l'écran produit sa propre lumière, aucun rétroéclairage n'est nécessaire. Cela réduit la puissance nécessaire pour faire fonctionner l'OLED et c'est pourquoi l'écran est si contrasté ; nous aimons vraiment cet écran miniature pour sa netteté ! La puce de pilote SSD1306, communique uniquement via I2C. 3 broches sont nécessaires pour communiquer avec la puce sur l'écran OLED, dont deux sont des broches d'horloge/données I2C. L'OLED et le pilote nécessitent une alimentation de 3,3 V et des niveaux logiques de 3,3 V pour la communication. Pour faciliter l'utilisation par nos clients, nous avons ajouté un régulateur de 3,3 V et un adaptateur de niveau à bord ! Cela le rend compatible avec n'importe quel microcontrôleur 5V, tel que l'Arduino. Les besoins en énergie dépendent un peu de la quantité d'énergie de l'écran qui s'allume, mais en moyenne, l'écran consomme environ 20 mA à partir de l'alimentation 3,3 V. Le pilote OLED intègre une simple pompe de charge qui transforme 3,3v-5v en un variateur haute tension pour les OLED [20].

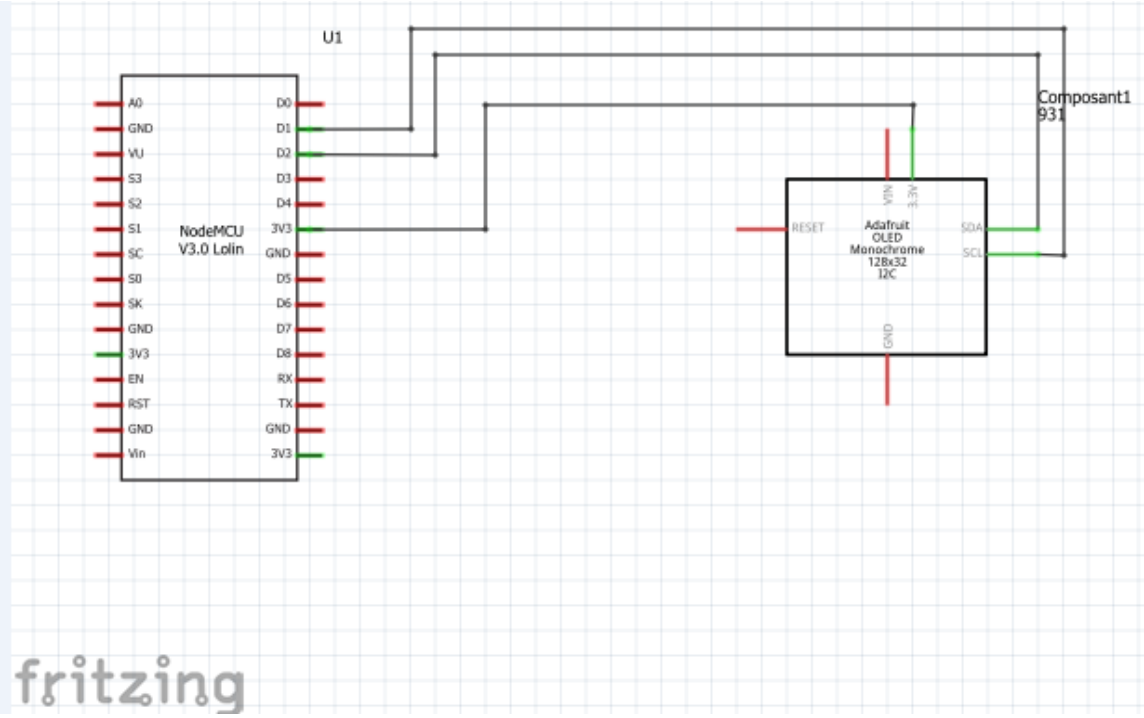

Figure31 ; Circuit microcontrôleur avec OLED

2.4 Le buzzer :

Ce composant électromagnétique ou piézoélectrique qui transforme l'énergie électrique en vibration, donc en son.

2.4.1 Le Buzzer actif : qui peut recevoir une tension continue. On le différencie du Buzzer passif, car l'électronique n'est pas apparent sur la face inférieure du buzzer. De plus le Buzzer actif possède souvent une étiquette sur le dessus.

Figure 32 : Buzzer actif

2.4.2 Le Buzzer passif : qui fonctionne avec une tension alternative, dont la fréquence est généralement comprise entre 500 Hz et 5 kHz. Comme expliqué sur la chaîne YouTube de U=RI (https ://www.youtube.com/watch ?v=HBHmCmjDpLA). Celui-ci fonctionnera donc sur une broche PWM.

On peut le reconnaitre aisément car sur la face du dessous (celle des broches) on peut voir les composants électroniques.

.

Figure 33 : Buzzer passif

Dans notre cas on à utiliser un buzzer actif qui fonctionne sous une tension varie entre 3V jusqu'à 24V[23].

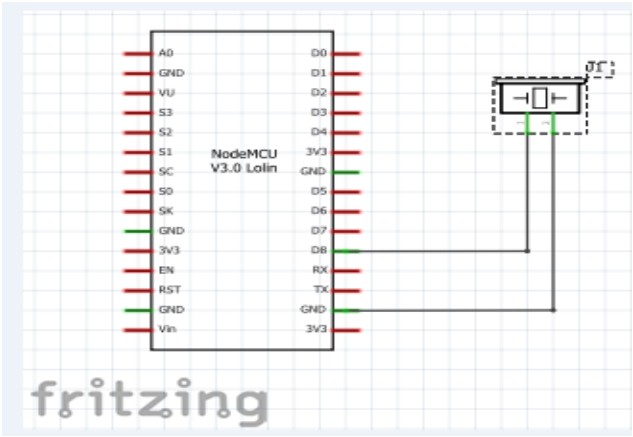

Figure 34 : Circuit microcontrôleur avec buzzer

2.5 Clavier numérique :

Ce clavier comprend 16 touches disposées en 4 lignes et 4 colonnes, L'appui sur une touche fait communiquer une ligne avec une colonne afin de livrer le code pin tapé par l'utilisateur au microcontrôleur [21].

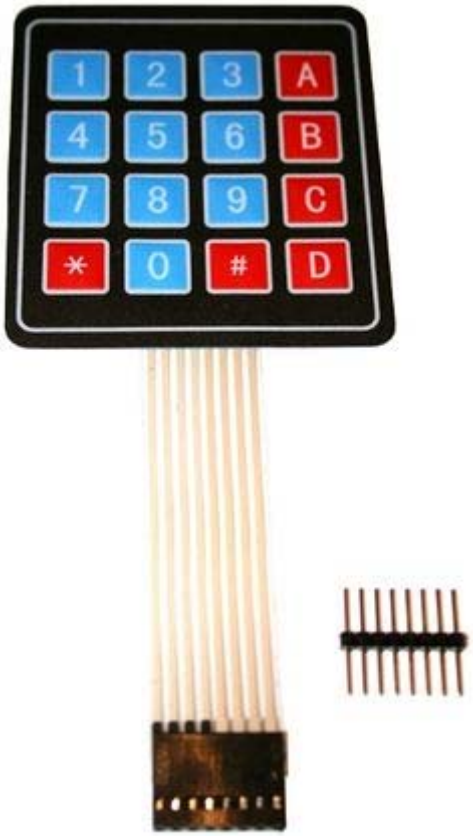

Figure35 : Pavé numérique 4x4

2.6 Le relais :

Un relais est un organe électrique permettant de dissocier la partie puissance de la partie commande. Il sert à faire une transition entre un courant faible et un courant fort. Il est constitué d'une bobine ou solénoïde qui lorsqu'elle est sous-tension attire par un phénomène électromagnétique une armature ferromagnétique qui déplace des contacts.[24] .

2.6.1 Avantage :

- Capacité de commuter aussi bien des signaux continus qu'alternatifs sur une large gamme de fréquences.
- Fonctionnement avec une dynamique considérable du signal commuté.
- Aucun ajout de bruit ou de distorsion.
- Résistance de contact fermé très faible (il est moins facile de trouver des valeurs aussi faibles avec des composants électroniques).
- Résistance de contact ouvert très élevée (il est moins facile de trouver des valeurs aussi élevées avec des composants électroniques).
- Très grande isolation entre circuit de commande (bobine) et circuit commuté (contacts).
- Possibilité de résoudre des problèmes d'automatisme de façon parfois plus simple qu'avec un circuit électronique

3. Software :

3.1 Fretzing :

C’est un logiciel open-source qui permet de créer des schémas électronique design et des schémas de circuit imprimés.

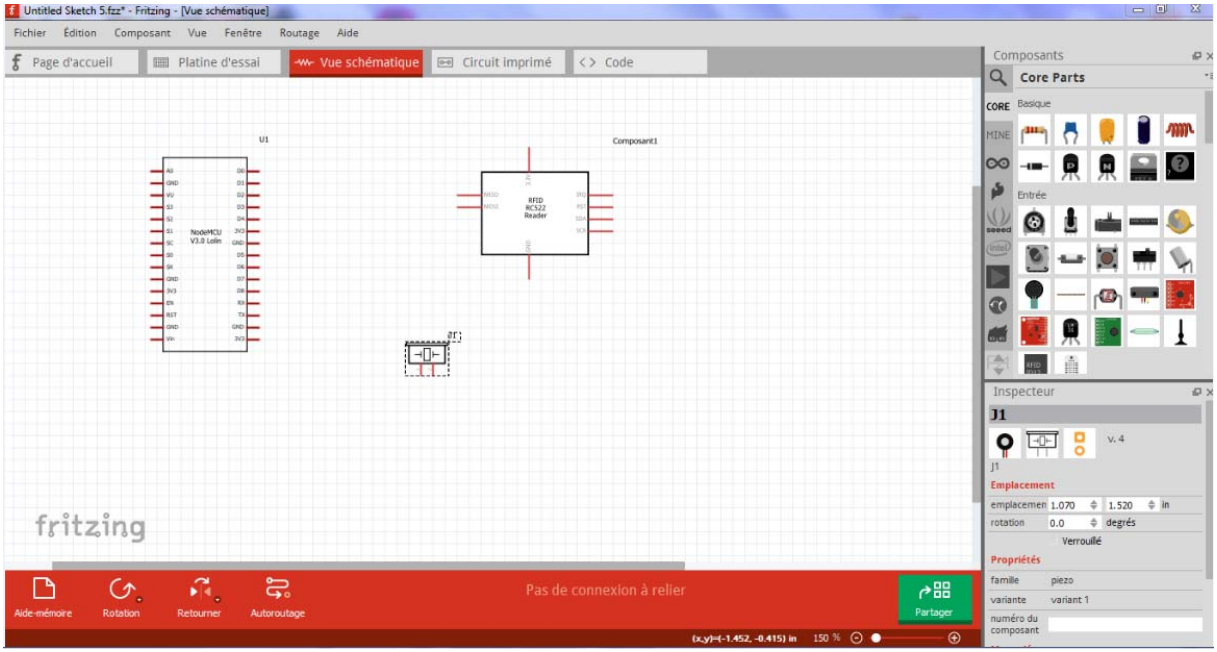

Figure36 : fretzing

3.2 Proteus professionnel 8 :

Proteus Professional est une suite logicielle destinée à l'électronique. Développé par la société L’absenter Electronics, les logiciels incluent dans Proteus Professional permettent la CAO (Construction Assistée par Ordinateur) dans le domaine électronique. Deux logiciels principaux composent cette suite logicielle : (ISIS, ARES, PROSPICE) et VSM.

Cette suite logicielle est très connue dans le domaine de l'électronique. De nombreuses entreprises et organismes de formation (incluant lycée et université) utilisent cette suite logicielle. Outre la popularité de l'outil, Proteus Professional possède d'autres avantages :

• Pack contenant des logiciels facile et rapide à comprendre et utiliser

• Le support technique est performant

• L'outil de création de prototype virtuel permet de réduire les coûts matériel et logiciel lors de la conception d'un projet

3.3 Wireshark :

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle GTK+ pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autres une version en ligne de commande nommé TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License.

3.4 Plateforme de surveillance d'accès :

C'est une application web qui vérifie l'historique d'accès de chaque personne et de télécharger un rapport complet sous format PDF ou de l'imprimer avec la possibilité de faire la gestion des personnels en ajoutant des nouveaux ou en supprimant ceux dont nous n'avons besoin.

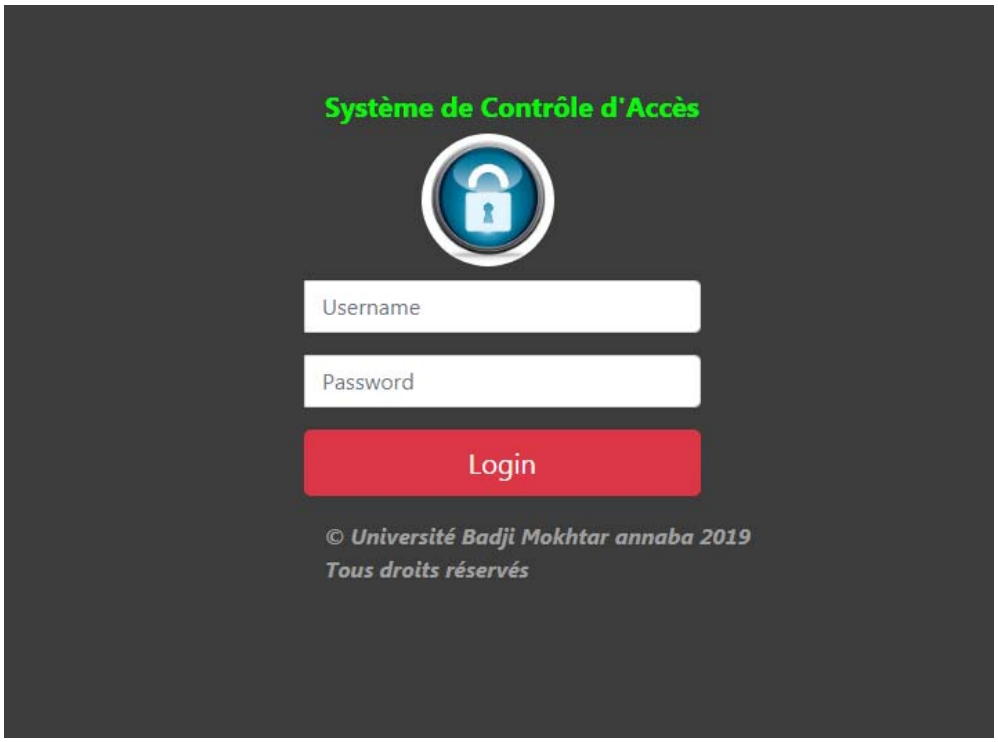

Figure37 : Login serveur

Après avoir effectué l'authentification l'administrateur pourrait bénéficier de toutes les fonctionnalités offertes.

Figure38 : La plateforme de contrôle et surveillance d'accès

3.5 Validation du système globale :

On va faire une démonstration du fonctionnement de système de surveillance et contrôle d'accès

L'utilisateur doit présenter son propre tag devant le lecteur

La serrure s'ouvre et le message « porte ouverte » s'affiche sur l'écran OLED avec l'enregistrement de l'accès dans la base de données.

4. Conclusion

Dans ce chapitre nous avons présenter la réalisation de notre système, en représentant quelques interfaces graphiques et en décrivant comment nous avons planifié notre projet.

Conclusion générale

Dans ce manuscrit nous avons présenter notre projet de fin d'étude qui consiste à système de contrôle et surveillance d'accès à base de la technologie RFID.

Le système conçu et réalisé de sécurité de contrôle d'accès est basé sur l'identification par radiofréquence a permis d'automatiser la tâche d'ouverture et de la fermeture des portes par l'utilisation d'un microcontrôleur et un lecteur RFID avec l'avantage de garder l'historique d'accès ainsi que la surveillance en temps réel à l'aide d'une application web qui sert comme une plateforme de contrôle de surveillance.

Ce projet nous a poussé à apprendre et à utiliser une grande panoplie d'outils comme programmer un microcontrôleur, le connecter à un réseau en utilisant la technologie WIFI, création échange de paquets http avec le microcontrôleur, etc.

Dans ce projet On a utilisé le logiciel Wirshark pour examiner les protocoles et les paquets en cours d'échange et surveiller le bon déroulement de la communication entre notre application web et le microcontrôleur.

Nous avons utilisé logiciel Fretzing dans la conception de notre circuit électronique parce qu'il est riche en composants nécessaires et convivial. Pour la simulation du système on a utilisé le logiciel Proteus professionnel qui nous a permis de tester le fonctionnement des composants.

L'utilisation de l'Arduino des cartes d'interfaces à grandement facilité la réalisation du système et nous a permis d'obtenir un résultat assez concluant.

Références :

[1]:application sur Technologie RFID Réalisé par : Mr YAHIAOUI Billal Mr SFAÏHI Ali

[2] :https://altec.ch/technologies/les-tags-rfid/

[3]:http://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158/

[4] ://www.commentcamarche.net/contents/520-le-protocole-http

[5]://www.academia.edu/5163800/Chapitre3._microcontroleur

[6]: https://www.academia.edu/5163800/Chapitre3._microcontroleur

[7]:http://www.composelec.com/communication_serie.php

[8] :https://www.metallerie-serrurerie.net/differents-types-de-serrures/

[9]: :http://clg-andre-chene-les-jacobins-fleury-les-aubrais.tice.ac-orleanstours.

fr/eva/sites/clg-andre-chene-les-jacobins-fleury-lesaubrais/

IMG/pdf/serrure_connectee.pdf Consulté le 15/03/2017

[10] : http://www.siloged.fr/cours/html/old_sysml2/le_diagramme_de_dfinition_de_bloc.html

[11] :https://www.google.com/search?q=qu%27est+ce+qu%27un+proteus+8+professional+pdf&safe=strict&ei=Z6PyXIzCKOqKjLsPyKOO0A4&start=10&sa=N&ved=0ahUKEwjMkfLu1cjiAhVqBWMBHciRA-oQ8tMDCIgB&biw=1366&bih=657

[12] : http://www.louisreynier.com/fichiers/KesacoArduino.pdf

[13] : https://laurent-audibert.developpez.com/Cours-UML/?page=diagramme-cas-utilisation

[14] :http://docwiki.embarcadero.com/RADStudio/Rio/fr/D%C3%A9finition_des_diagrammes_d%27activit%C3%A9s_UML_2.0

[15] : https://fr.wikipedia.org/wiki/Diagramme_de_s%C3%A9quence.

[16]:http://www.uml-sysml.org/diagrammes-uml-et-sysml/diagramme-uml/diagramme-de-classe

[17] ; https://www.moussasoft.com/product/module-rfid-rc522-lecteur-rfid

[18] ://framboiseaupotager.blogspot.com/2017/12/lessentiel-sur-esp8266-nodemcu-sequence.html

[20]:https://boutique.semageek.com/fr/1372-ecran-graphique-monochrome-128x32-i2c-oled.html

[21]:http://colmard.com/Arduino-lecon25.html

[23] : https://ardwinner.jimdo.com/arduino/viia-les-capteurs/1a-buzzer-alarme/

{24] : https://www.researchgate.net/figure/9-Description-dun-relais-electromagnetique-512-Relai-electromagnetique-Comme-son-nom_fig26_321533642

Annexe A :

Le circuit global du système de surveillance et contrôle d'accès :