REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Larbi Ben M'hidi - Oum El bouaghi Faculté des Sciences et des Sciences Appliquées Département de génie électrique

Filière d'Électronique



MEMOIRE DE FIN D'ETUDES

En vue de l'obtention du diplôme de

Master Académique

Spécialité : Electronique des systèmes embarqués



Etude et réalisation d'un système de contrôle d'accès sécurisé à base de la technologie RFID

Mémoire de fin d'études, soutenu publiquement À Oum El Bouaghi, le 27/10/2020

Présenté par

Kenza MESSOUD DEBBIH

- Samouna ZERROUKI

Dirigé par

Dr. Souheil MOUETSI

Jury de soutenance

Président : LASHAB Mohamed Pr Université Mohamed Larbi

Encadreur : MOUETSI Souheil Pr Ben M'hidi – Examinateur : CHIHA Yamina MAA Oum El bouaghi

Année universitaire: 2019/2020



Remerciements



Notre remerciement Avant tout, louange à «ALLAH»

qui nous a donnés la force et la patience de finaliser ce modeste Travail.

Nous remercions considérablement notre encadreur Monsieur:

Mouetsi Souheil

Qui nous a chaleureusement accueillis

et a accepté de diriger ce mémoire, et qui était toujours disponible, dont les encouragements et les conseils judicieux de très grande utilité.

Nous remercions les membres de jury, chacun par

Son nom, qui nous ont honorés en acceptant d'examiner notre travail.

Nous tenons à remercier sincèrement reconnaissances à tous les enseignants

Du département de génie électronique

de l'université Mohamed larbi ben m'hidi d'Oum el bouaghi.

Nous adressons nos sincères remerciements à tous ceux qui ont contribué,

de près ou de loin, à la réalisation de ce travail.

Enfin, nous remercions tous nos amis



Kenza. M $\mathcal L$ Samouna. $\mathcal Z$

Dédicace



Nous tenons tout d'abord à remercier Dieu le tout puissant qui nous a donné la force et la patience d'accomplir ce Modeste travail.

C'est un plaisir de dédier notre travail à ceux qui ont été une source d'inspiration,

de volonté et d'encouragement au cours de nos études

et nous remercions : Nos familles

Nos frères et nos sœurs

Tout nos amis de groupe ESE

Tous nos maitres et professeurs:

Du primaire au L'université

Aux bonnes personnes que nous avons rencontrées

dans notre vie

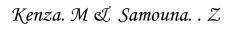


Table des matières

Liste de	es figures	3
Liste de	es Tableau	4
Introdu	ction générale	5
Chapit	re I : Systèmes de pointage et de contrôle d'accès	6
I. 1.	Introduction	6
I. 2.	Pourquoi utiliser un système de contrôle d'accès ?	6
I. 3.	Les différents systèmes de pointage	8
I. 4.	Les différents types d'un système de contrôle d'accès biométrique	10
I. 5.	Les différentes technologies d'identification	13
I. 6.	Composants des systèmes RFID	
I. 7.	Principe de fonctionnement de la RFID	16
I. 8.	Les caractéristiques des tags RFID.	17
I. 9.	Capteur RFID intégré	18
I. 10.	Principe de la modulation RFID	
I. 11.	Applications et domaines des cartes à puces	
I. 12.	Avantages et inconvénients de la technologie RFID	
I. 13.	Conclusion	22
Chapit	re II : Matériel utilisé	23
II. 1.	Introduction	23
II. 2.	Unité de commande et de traitement	23
II. 2. 1.	La carte Arduino UNO	23
II. 2. 2.	Module RFID	27
II. 3.	Unité de sortie et de communication (Afficheur LCD)	28
II. 3. 1.	Brochage d'un afficheur LCD.	29
II. 3. 2.	Principe de fonctionnement d'un écran LCD	
II. 4.	Unité d'entrée	31
II. 4. 1.	Clavier matriciel	
II. 5.	Composants auxiliaires	
II. 5. 1.		
	Servomoteur	
II. 6.	Conclusion	33
Chapit	re III : Réalisation d'un système de contrôle d'accès sécurisé	36
III. 1.	Introduction	36
III. 2.	Partie simulation	36
III. 3.	Câblage de montage	
	.Câblage de LED	
	.Câblage module RFID (RC-522)	
	. 3.Câblage d'un afficheur LCD	
	.Câblage de servomoteur	
	Logiciel (IDE Arduino)	
	La macro PLX-DAQ	
a)	Partie Arduino	
b)	Partie Excel	
III. 3. 7	$\boldsymbol{\varepsilon}$	
III. 3. 8		
	La partie expérimentale	47 47
	NATIONAL PROPERTY OF THE PROPE	-T /

Conclusion générale	48
Bibliographie	
Résumé	52

Liste des figures

Figure I.1: Feuille de pointage	8
Figure I. 2: Le contrôle d'accès mécanique	8
Figure I. 3: Le contrôle d'accès mobile	9
Figure I. 4: Badgeuse	9
Figure I. 5: Le contrôle d'accès biométrique	10
Figure I. 6 : Différents types de contrôle d'accès biométrique	10
Figure I. 7: Contrôle d'accès biométrique	11
Figure I. 8: Le contrôle d'accès d'empreinte digitale	12
Figure I. 9 : Caractéristiques du visage	12
Figure I. 10: Etiquettes (tag) à radiofréquence	15
Figure I.11 : Différents type de lecteur RFID	16
Figure I.12: Fonctionnement d'un tag RFID	17
Figure I.13 : Echange de données entre un lecteur et un tag RFID	17
Figure I.14 : Principales caractéristiques d'un tag RFID	18
Figure II. 1: La carte Arduino UNO	23
Figure II. 2: Les E/S d'une carte Arduino UNO	
Figure II. 3: Anatomie d'une carte Arduino UNO	25
Figure II. 4 : Schéma simplifié de la carte Arduino UNO	25
Figure II. 5 : Brochage de Microcontrôleur ATMega328	
Figure II. 6: lecteur RFID aves ses accessoires	28
Figure II. 7: Afficheur LCD et accessoires associées	
Figure II. 8 : Brochage d'un écran LCD	
Figure II. 9: Principe de fonctionnement d'un écran LCD	
Figure II. 10 : Clavier matriciel	
Figure II. 11: Buzzer 1. Electromécaniques 2. Piézo-électrique	
Figure II.12: Servomoteur	
Figure III.1: Organigramme de fonctionnement	
Figure III. 2 : Schéma synoptique du système	
Figure III. 3: Montage carte Arduino +LED	
Figure III. 4: Montage carte Arduino + lecteur RFID	
Figure III.5: Montage carte Arduino + afficheur	
Figure III.6: Montage carte Arduino +lecteur RFID + servomoteur	
Figure III.7: Logo Arduino	
Figure III.8: Logiciel (IDE Arduino)	
Figure III.9: logo PLX-DAQ-v2.11 Excel	
Figure III.10 : Acquisition des données à partir de fichier Excel	
Figure III.11: Exemple de lecture de fichier Excel	
Figure III. 12: Montage de simulation	
Figure III .13: Le schéma général (Fritzing)	
Figure III.14 : Montage expérimental	47

Liste des tableaux

Tableau I. 1 : Comparaison des différents types de technologie d'identification automatique	14
Tableau II. 2 : Rôle et nom de chaque broche d'un afficheur LCD	30

Introduction générale

Introduction générale

Le contrôle d'accès signifie les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à un bâtiment ou un site, ou les accès logiques à un système d'information. Les systèmes de contrôle d'accès sont des systèmes couramment utilisés pour marquer la présence dans les parkings, bureaux et les lieux de travail. Ces systèmes se sont considérablement améliorés, allant du marquage manuel des présences dans les registres de présence à l'utilisation d'applications de haute technologie. Lorsque nous parlons d'un système de contrôle d'accès physique, nous faisons généralement référence à un système de sécurité électronique. Ce dernier utilise généralement un identifiant, qui peut se présenter sous forme de badge d'accès, pour autoriser les personnes à pénétrer dans certaines zones. Et, comme le système est capable d'enregistrer qui est entré où et quand, il peut par la suite fournir des données précieuses pour nous aider à suivre l'utilisation de nos locaux et sites.

Dans ce projet, nous avons réalisé un système de contrôle d'accès on utilisant le module RFID (Radio Frequency Identification) via la carte Arduino pour contrôler l'accès en deux étapes : l'une en vérifiant le badge RFID et le second par l'introduction d'un code personnel à travers un clavier matriciel, à la fin, notre système permet d'enregistrer la liste de présence.

A signalé que notre projet de fin d'étude avant la pandémie de coronavirus est l'étude et réalisation d'une pointeuse biométrique avec lecture d'empreintes digitales, et vu le manque de matériel, nous avons changé notre sujet pour le contrôle d'accès à base de la technologie RFID.

Le présent mémoire est divisé en trois chapitres :

- Le premier chapitre présentera les différents systèmes de contrôle d'accès on commençant par les systèmes biométriques jusqu'à la technologie RFID on se basant sur les différents domaines d'utilisation, leurs principe de fonctionnement et les fréquences de communication utilisées.
- Le deuxième chapitre sera dédié à l'étude des différentes éléments de notre carte électronique y compris essentiellement la carte ARDUINO UNO et le module RFID.
- Le dernier chapitre sera consacré à la présentation de notre système de sécurité et les différentes étapes de programmation (codes utilisés) et câblage.

Enfin, nous terminerons notre mémoire avec une conclusion générale.

Chapitre I

Système de pointage et contrôle d'accès

Chapitre I : Systèmes de pointage et de contrôle d'accès

I. 1. Introduction

Un système de pointage est un simple outil de mesure et de contrôle du temps de travail, elle doit répondre aux besoins de l'employeur en termes d'organisation du temps de travail dans son entreprise.

Le pointage est un dispositif qui permet de contrôler le temps de travail d'un salarié. A l'origine, les horaires et accès spécifiques à une zone étaient contrôlés par un salarié qui notait scrupuleusement chaque aller et venue d'un salarié.

Dans ce chapitre, nous traitons des différentes questions relatives au système de contrôle d'accès plus particulièrement la technologie RFID (Radio Frequency Identification), nous donnons aussi une succincte définition, son principe de fonctionnement, ses avantages et ses inconvénients, présentation d'un large éventail d'applications dans plusieurs domaines.

I. 2. Pourquoi utiliser un système de contrôle d'accès ?

Selon le cas on utilise un système de contrôle d'accès, on peut citer les avantages de tel système. Par exemple dans une entreprise, le salarié doit accéder rapidement à son poste de travail, et son temps de travail doit être mesuré précisément. Selon le secteur d'activité, le contrôle d'accès permet également de faire gagner du temps à l'équipe de la gestion paie, qui n'aura qu'à vérifier rapidement les cohérences des informations pour établir à l'aide d'un logiciel de pointage les documents sociaux du salarié, comme son bulletin de salaire. En résumé, l'installation d'un tel système fera gagner un temps conséquent en facilitant les opérations du décompte des horaires de présence.

En pratique, les différents systèmes de pointage présentent beaucoup d'avantages, mais dans les faits, ils doivent répondre à un cadre légal et juridique très précis [1].

Souvent synonyme de flicage, la mise en place d'un tel système de contrôle d'accès horaire en entreprise est mal perçue. Pourtant, cela apporte de nombreux avantages à l'entreprise, mais aussi aux salariés.

1) Limiter les conflits

Avec un système totalement impartial, on limite naturellement les conflits liés aux horaires. Le contrôle d'accès fait foi et atteste la présence ou de l'absence d'un salarié, de l'heure à laquelle il arrive et il repart. En cas de litige, il sera simple de produire des documents contenant les informations exportées par le système [2].

2) Optimiser l'organisation

Le contrôle d'accès permet de mieux cerner l'activité de son entreprise, les temps de présence, d'absence, etc. L'objectif, en utilisant un logiciel de gestion du temps, est d'avoir une vision globale qui permet, à terme, de mettre en place des plannings optimisés pour une meilleure organisation et donc, une plus grande rentabilité [2].

3) Limiter les tâches administratives

C'est au niveau de service comptabilité que l'on apprécie particulièrement cet outil de contrôle d'accès. De fait, oubliez les post-it sur lesquels les salariés notaient leurs horaires, aujourd'hui toutes les informations sont exportées automatiquement. Gestion du temps de travail, des heures supplémentaires, des présences, absences, etc., tout est automatisé. Cela offre un gain de temps conséquent et donc, un gain de productivité [2].

4) Mieux connaître l'activité de son entreprise

Les managers peuvent s'apercevoir des horaires réellement réalisés par leurs équipes. De fait, cela met en lumière certaines pratiques qui engendrent des heures supplémentaires parfois conséquentes. Prenons un exemple concret avec un employé dont les horaires sont 5h-13h en usine. S'il travaille réellement jusqu'à 13h, avant de pointer, il va se rendre au vestiaire pour se changer.

Il va donc pointer à 13h10 ou 13h15, cela engendre à l'année un nombre important d'heures supplémentaires et donc un coût. Un logiciel de gestion du temps met immédiatement en lumière cet aspect et donne la possibilité d'y remédier, notamment en faisant en sorte que les employés finissent leur travail 10 minutes plus tôt. Le coût sera moins important puisqu'il s'agit d'horaires non majorés [2].

5) Plus fiable pour les salariés

Comme évoqué ci-dessus, il n'aura plus besoin de noter les horaires d'un salarié, au risque de perdre ses informations. De fait, chaque minute passée dans l'entreprise est comptabilisée pour un calcul plus juste des salaires et des congés [2].

I. 3. Les différents systèmes de pointage

Il existe différents systèmes de pointage :

1) Feuille de pointage : c'est l'enregistrement papier ou numérique des données fournies par le contrôle d'accès. Elle peut aussi être remplie manuellement et constituer à part entière un moyen de contrôle du temps de travail [3].

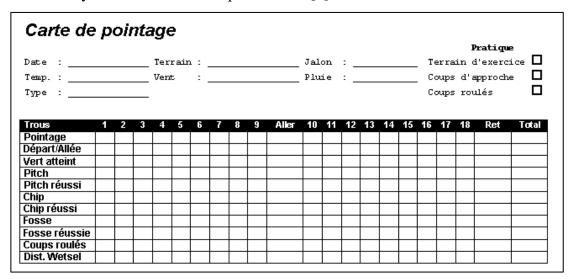


Figure I.1 : Feuille de pointage

2) Le contrôle d'accès mécanique : ce système doté d'une horloge permet de connaître les heures d'arrivée et de départ du personnel via l'insertion d'une carte ou la pression d'un bouton. Le contrôle d'accès mécaniques (ou numériques) permettent aux salariés d'insérer un support (carton ou carte plastique) qui servira notamment de rappel d'identité, et sur lequel est noté de manière informatisée les horaires d'arrivée, de pauses et de départ de l'entreprise [1].



Figure I. 2 : Le contrôle d'accès mécanique

3) Le contrôle d'accès mobile : ce système de pointage permet de contrôler le temps de travail des salariés non sédentaires et passant une partie importante de leur temps en dehors des locaux de l'entreprise. Ainsi, le gain de temps et la simplicité d'utilisation favorise la productivité de certains secteurs [3].



Figure I. 3 : Le contrôle d'accès mobile

4) Badgeuse : c'est une évolution de la carte à insérer dans la le contrôle d'accès. Il s'agit désormais d'un badge à insérer dans un système de contrôle d'accès, les données sont ensuite enregistrées et traitées automatique [3].



Figure I. 4: Badgeuse

5) Le contrôle d'accès biométrique : il s'agit du système de pointage le plus évolué, car il permet d'enregistrer des données physiologiques comme les empreintes digitales, le fond de l'œil par exemple [3].



Figure I. 5 : Le contrôle d'accès biométrique

I. 4. Les différents types d'un système de contrôle d'accès biométrique

Le contrôle d'accès biométrique réagit en déclenchant un décompte des horaires de travail quand un de ses capteurs (caméra, pad, etc.) reconnaît une caractéristique humaine comme :

- des empreintes digitales.
- Le contour d'une main.
- Un visage.
- Un iris
- Modulo RFID ... [9]

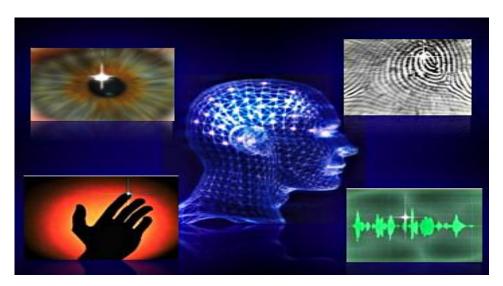


Figure I. 6 : Différents types de contrôle d'accès biométrique

1) Le contrôle d'accès d'empreinte digitale

Les empreintes digitales sont le dessin formé par les lignes de la peau des doigts, ils sont appelées aussi dermatoglyphes, ce sont une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu ; c'est ce qui motive leur utilisation par la police criminel d'empreinte digitale depuis le 19^{ème} siècle [7].



Figure I. 7: Contrôle d'accès biométrique

On distingue deux types d'empreintes :

- l'empreinte directe ou visible qui laisse une marque visible à l'œil nu,
- l'empreinte latente ou invisible qui est composée de lipides, de sueur et de saletés déposés sur un objet touché.

Ce type de pointage biométrique permet un accès simple au lieu de travail. L'employé peut pointer en utilisant son doigt seulement, sans carte ni badge.

Cette solution de pointage facilite le travail des gestionnaires de ressources humaines en contrôlant toutes les entrées / sorties de façon très simple, par le rapatriement des données via une clé USB par exemple [7].

2) Le contrôle d'accès avec un contour d'une main

La géométrie de la main est une technologie biométrique récente. Comme son nom l'indique, elle consiste à analyser et à mesurer la forme de la main, c'est - à - dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur et de créer une image 3D. Des LEDs infrarouges et un appareil photo numérique sont utilisés pour acquérir les données de la main



Figure I. 8 : Le contrôle d'accès d'empreinte digitale

Cette technologie offre un niveau raisonnable de précision et il est relativement facile à utiliser. Cependant, elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proches. Les utilisations les plus populaires de la géométrie de la main comprennent l'enregistrement de présence et le contrôle d'accès. Par contre, les systèmes de capture de la main sont relativement grands et lourds, ce qui limite leur utilisation dans d'autres applications comme l'authentification dans les systèmes embarqués : téléphones portables, voitures, ordinateurs portables [8].

3) Le contrôle d'accès avec les contours de visage

Rien n'est plus naturel qu'utiliser le visage pour identifier une personne. Les images faciales sont probablement la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.

L'utilisation d'une caméra permet de capter la forme du visage d'un individu et d'en dégager certaines particularités. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence [7].

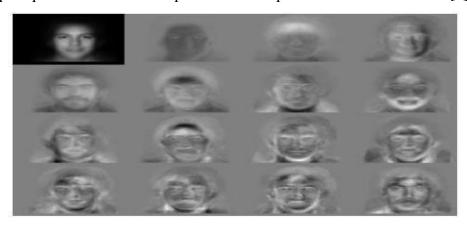


Figure I. 9 : Caractéristiques du visage

4) Le contrôle d'accès d'iris

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification.

L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de l'individu est à une distance fixe et proche du dispositif de capture, ce qui limite l'utilisation de cette technologie [8].

5) La technologie RFID

La technologie d'identification par radiofréquence (Radio Frequency Identification RFID) est une technologie de capture automatique de données basées sur les ondes et rayonnements radiofréquence, elle est formée de trois composantes : une étiquette (ou plusieurs étiquettes), un lecteur ou un interrogateur ainsi que l'infrastructure de soutien correspondante (soit les composantes matérielles et les logiciels nécessaires) [10].

I. 5. Les différentes technologies d'identification

L'identification automatique se fait par plusieurs types de technologies. Dans ce présent travail, nous n'allons pas nous étendre sur tous les différents types de technologies, mais nous allons présenter quelques-uns à l'instar des codes à barres, des cartes intelligentes, des RFID passives et actives ainsi que les lecteurs d'empreintes.

- Les codes à barres : sont destinés à automatiser l'acquisition d'une information généralement numérique. Ils trouvent leurs applications dans différents domaines comme la gestion des prêts d'une bibliothèque, les caisses enregistreuses, etc.
- L'étiquette RFID passive : comme son nom l'indique, les tags passifs attendent un signal d'un lecteur RFID. Le lecteur envoie de l'énergie à une antenne qui convertit cette énergie en une onde RF qui est envoyée dans la zone de lecture. (Nous allons le détailler dans le paragraphe qui suit) [11].

- L'étiquette RFID active : comme les systèmes RFID passifs, les systèmes RFID actifs sont composés de lecteurs, d'étiquettes et d'antennes. Cependant, les systèmes passifs exigent que les étiquettes soient activées par le lecteur, les systèmes RFID actifs utilisent des étiquettes RFID alimentées par batterie qui ne nécessitent pas d'énergie pour envoyer un signal [12].
- Le lecteur d'empreinte : est parfait pour les gestionnaires RH (Ressource Humaine) de toute entreprise petite ou moyenne. Ce lecteur d'empreintes digitales fera des merveilles et facilitera le travail en permettant de suivre de plus près le temps des employés [13].

Sur le tableau ci-dessous, nous présentons une étude sur les différentes technologies d'identification automatique en faisant une comparaison sur leurs avantages et leurs inconvénients [14].

Technologies	Modification Des données	Sécurité de données	Volume de données	Coûts	Durée de vie
Codes à barres	Non modifiable	Minimale	Codes a barre linéaire contient 8-30 bytes. Certains codes a barre a 2D contient jusqu'a 7200 bytes.	Bas	Court
Etiquettes RFID active	Modifiable	Haute	Jusqu'à 8 MB	Très élevé	3-5 ans
Etiquettes RFID passive	Modifiable	Moyenne	Jusqu'à 64 KB	Moyen	Indéfini
Lecteurs d'empreintes	Non modifiable	Moyenne	certains lecteurs peuvent mémoriser jusqu'à 9000 empreintes.	Moyen	/
Carte intelligente	Modifiable	Haute	Jusqu'à 8 MB	Elevé	Long

Tableau I.1 : Comparaison des différents types de technologie d'identification automatique

Après avoir fait cette comparaison nous nous sommes penchées sur la technologie RFID. Une technologie qui nous semble être la mieux adaptée par rapport aux avantages qu'elle présente et à sa facilité d'utilisation.

I. 6. Composants des systèmes RFID

Pour pouvoir mettre en place un système de traçabilité RFID, nous devons avoir un équipement spécifique composé de :

I. 9. 1. L'étiquette (tag)

C'est un dispositif récepteur, que l'on place sur des éléments (objet, animal...). Ils sont munis d'une puce contenant les informations et d'une antenne pour permettre les échanges d'informations. La figure ci-dessous, montre une étiquette à radiofréquence qui se compose d'une puce et d'une antenne.



Figure I. 10: Etiquettes (tag) à radiofréquence

I. 9. 2. Le lecteur RFID

Le lecteur/enregistreur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et d'une électronique qui reçoit et décode les informations envoyées par l'étiquette et les envoie au dispositif de collecte des données. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence et de la transmission des informations qu'elle ; s contiennent.



Figure I.11 : Différents type de lecteur RFID

I. 7. Principe de fonctionnement de la RFID

Un système RFID est composé de deux entités qui communiquent entre elles :

- Un tag ou étiquette intelligente (aussi appelé transpondeur), associé à l'élément à identifier. Il est capable de répondre à une demande venant d'un lecteur.
- Une station de base ou lecteur RFID qui a pour mission d'identifier le tag. le lecteur envoie une onde électromagnétique en direction de l'élément à identifier. En retour, il reçoit l'information renvoyée par le tag.

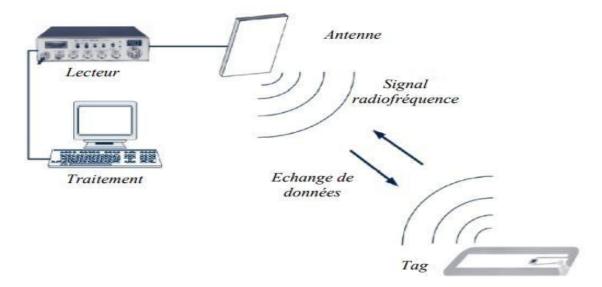


Figure I.12: Fonctionnement d'un tag RFID

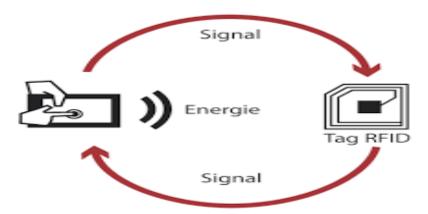


Figure I.13 : Echange de données entre un lecteur et un tag RFID

I. 8. Les caractéristiques des tags RFID

Etablir une classification complète de la technologie RFID est difficile étant donné le nombre de caractéristiques qui doivent être considérées pour définir un tag. C'est uniquement lors de la conception d'une application RFID qu'il est possible de définir les besoins technologiques et par la suite, d'identifier le type de tag le plus approprié. Les principales caractéristiques des tags RFID sont représentées sur la figure ci-dessous [17].

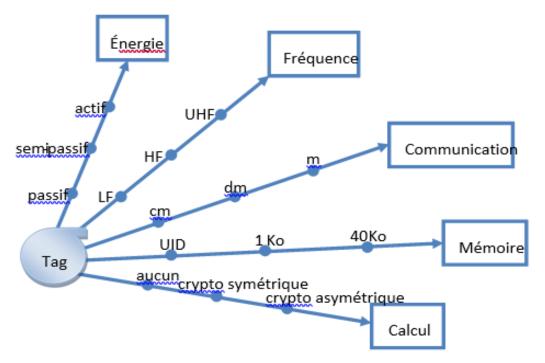


Figure I.14: Principales caractéristiques d'un tag RFID

I. 9. Capteur RFID intégré

Un appareil électronique qui produit un signal électronique en réponse à une stimulation physique. Les capteurs sont plus fréquemment intégrés dans des étiquettes RFID. Comme exemple, nous avons le contrôle de température d'un article. Le capteur peut être intégré à n'importe quelle classe d'étiquettes (passives, semi-passives et actives). On distingue :

I. 9. 1. L'étiquette capteur RFID

L'étiquettes-capteur RFID (Sensor enabled RFID tag ou "sensor tag") est une étiquette RFID qui contient un capteur pour surveiller un certain paramètre physique (par exemple, la température) mais contient également la même la fonction d'identification qu'une étiquette « normale » de RFID. Ce genre d'étiquette-capteur peut être de classe 2, classe 3 ou classe 4 dans la classification de l'étiquette d'EPC global [18].

Comme entièrement passive, une étiquette de la classe 2 peut mesurer des paramètres physiques seulement une fois mise sous tension par l'interrogateur. Puisque la classe 3 des étiquettes a une batterie, les capteurs peuvent travailler indépendamment. Par conséquent, ils peuvent contenir des dispositifs de notation pour maintenir des résultats de mesure en fonction du temps où ils peuvent enregistrer des événements prédéfinis. L'avantage de la classe 4 est la fiabilité accrue de lecture.

I. 9. 2. Capteurs RFID

Les capteurs sont des dispositifs qui transforment des quantités physiques telles que la pression ou l'accélération en signaux de sortie (habituellement électriques) pour servir d'entrées pour contrôler le système» [19].

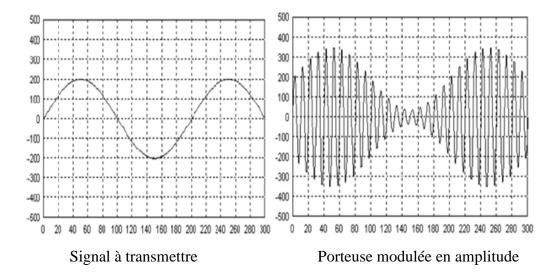
Le développement rapide de la technologie de RFID présente une occasion neuve pour évoluer l'application de capteurs. Les étiquettes RFID qui portent des capteurs qui peuvent être employées dans des domaines tels que le cheminement de projet, le contrôle de l'environnement, système électronique des véhicules à moteur, télémédecine et le contrôle de processus, etc., sont multipliés comme résultat. Les capteurs primaires en service aujourd'hui peuvent être classifiés selon leurs fonctions comme capteur :

- de température
- de pression
- d'accélération
- d'inclination
- d'humidité
- de lumière
- Capteurs de gaz
- Capteurs chimiques

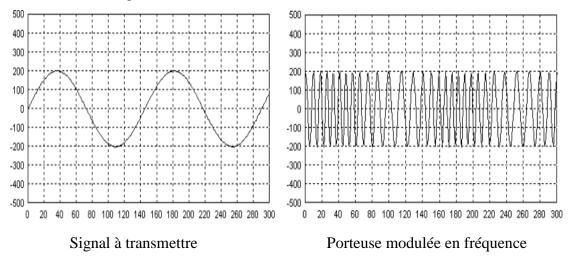
I. 10. Principe de la modulation RFID

En RFID, les dispositifs qui communiquent ne sont pas technologiquement conçus de la même façon. Pour cette raison, des types de modulation différents sont utilisés selon le sens de la communication [20].

Les modulations les plus couramment utilisées sont :



- Modulation d'amplitude : Dans ce type de modulation, la porteuse est modulée en amplitude, c'est-à-dire que des variations d'amplitude de ce signal permettent de traduire le message à transmettre.
- Modulation de fréquence : Dans ce type de modulation, la porteuse est modulée en fréquence, c'est-à-dire que des variations de fréquence de ce signal permettent de traduire le message à transmettre.



I. 11. Applications et domaines des cartes à puces

Les cartes à puce ainsi que les badges RFID servent dans de multiples domaines Les cartes à puce sont utilisées dans les systèmes de paiement comme les cartes bancaires, mais aussi sous forme de carte SIM en téléphonie. On dénombre beaucoup de possibilités d'utilisation des cartes à puce dans le contrôle d'accès afin d'identifier les individus que ce soit pour entrer dans un bâtiment, une pièce ou pour se connecter à un ordinateur via un contrôle d'accès logique.

Au quotidien nous utilisons énormément de cartes à puce sans y faire attention. Notre téléphone fonctionne avec une carte SIM, les puces sont partout et nous accompagnent au quotidien [21] :

- Monétique / paiement
- Téléphonie
- Identification
- Santé
- Sécurité
- Transport
- Authentification
- Logistique
- Traçabilité

Ils peuvent notamment servir dans les payés développées en :

- Contrôle d'accès : porte-clés d'accès
- Abonnement : carte de membre
- Titre de transport : carte de bus et tramway
- Fidélité : carte de fidélité
- Restaurants administratifs : carte de self
- Carte d'identité
- Passeport
- Suivi de stocks : tag RFID
- Serrure électronique
- Piscine / SPA : bracelets d'accès / bracelet de casier
- Salle de sport : bracelet RFID
- Club de forme
- Bibliothèque : carte de bibliothèque, carte de médiathèque
- Camping
- Festival: carte cashless, bracelet sans contact
- ...

I. 12. Avantages et inconvénients de la technologie RFID

a) Avantages

- Lecture et décodage instantanée.
- Remplacement de la saisie au clavier.
- Facilité de branchement (écran clavier) et l'utilisation du lecteur optique.
- Coût abordable.

b) Inconvénient

- Faible capacité.
- Impossibilité de modifier les informations.
- Exigence d'un contact visuel pour la lecture.
- Impossibilité de lecture simultanée.
- Contenu non évolutif [22].

I. 13. Conclusion

Dans le premier chapitre nous avons présenté le système de contrôle d'accès et de pointage. Ensuite, nous avons focalisé notre étude sur la technologie RFID ou l'identification par radiofréquence, cette technologie est de systèmes sans fil permettant une lecture d'information sans contact. Ce type de système fonctionne sur la base des informations et données qui sont collectées des étiquettes par de lecteurs spécifique. Nous avons également présenté, le principe de fonctionnement de la technologie RFID, ses avantages et inconvénients ainsi les différentes domaines d'applications.

Chapitre II: Matériel utilisé

II. 1. Introduction

L'objective de notre travail consiste à l'étude et réalisation d'un système de contrôle d'accès à base de la technologie RFID et la saisie d'un code personnel d'identification pour la reconnaissance des individus. Dans ce chapitre, nous présentons l'ensemble des composants nécessaire pour notre projet :

- Unité de commande et de traitement : Arduino UNO.
- Unité de sortie et de communication : Afficheur LCD.
- Unité d'entrée : un clavier électronique et le module RFID.
- En plus, d'autres composants auxiliaires tel que : le Buzzer et l'horloge RTC.

II. 2. Unité de commande et de traitement

II. 2. 1. La carte Arduino UNO

C'est une petite carte électronique $(5,33 \times 6,85 \text{ cm})$ équipée d'un microcontrôleur, ce dernier permet, à partir des d'événements détectés par des capteurs, de programmer et de commander des actionneurs ; la carte Arduino est donc une interface programmable [23].



Figure II. 1: La carte Arduino UNO

Le modèle UNO de la société ARDUINO est une carte électronique dont le cœur est un microcontrôleur ATMEL de référence ATMega328. Le microcontrôleur ATMega328 est un microcontrôleur 8bits de la famille AVR dont la programmation peut être réalisée en langage C [24].

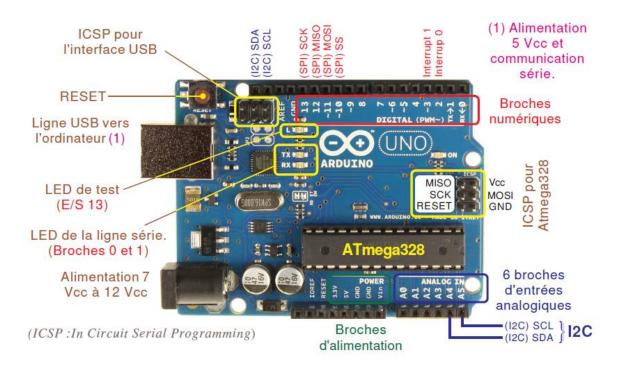


Figure II. 2: Les E/S d'une carte Arduino UNO

II. 2. 1. 1. Caractéristiques techniques de la carte Arduino UNO [23]

- Microcontrôleur : ATmega328.
- Fréquence horloge : 16 MHz.
- Tension d'alimentation interne : 5Vcc.
- Tension d'alimentation externe recommandée : 7-12Vcc. (Limites : 6-20 Vcc)
- Courant max sur la sortie 3,3V généré par le régulateur interne : 50mA.
- Entrées/sorties binaires : 14 broches.
- Courant MAX par broches en sortie : 40 mA. (85 mA en court-circuit)
- Courant MAX cumulé par les broches en sorties : 200 mA. (Soit 14 mA en moyenne)
- Les E/S binaires 0 et 1 sont mobilisées par le dialogue sur la ligne série.
- S0 pour RX et S1 pour TX. Chaque broche est reliée à une LED via $R = 1k\Omega$.
- Les E/S binaires 3, 5, 6, 9, 10, et 11 sont dédiées au mode PWM.
- L'E/S 13 est reliée sur la carte à la LED de test via une résistance de 1kΩ.
- Entrées analogiques : 6, le niveau logique maximal doit être de +5Vcc.
- Mémoire Flash 32 KB dont 0.5 KB utilisée par le Boot loader.
- Mémoire SRAM 2 KB, Mémoire EEPROM 1 KB.
- La carte s'interface au PC par l'intermédiaire de sa prise USB.
- La carte s'alimente par le jack d'alimentation.

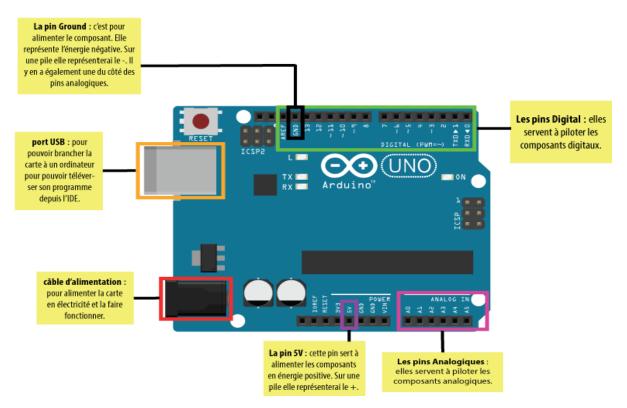


Figure II. 3: Anatomie d'une carte Arduino UNO

II. 2. 1. 2. Schéma simplifié de la carte Arduino UNO

Le microcontrôleur utilisé sur la carte Arduino UNO est un microcontrôleur ATMega328, ce dernier est un circuit intégré qui rassemble sur une puce plusieurs éléments complexes dans un espace réduit dont la programmation peut être réalisée en langage C [25].

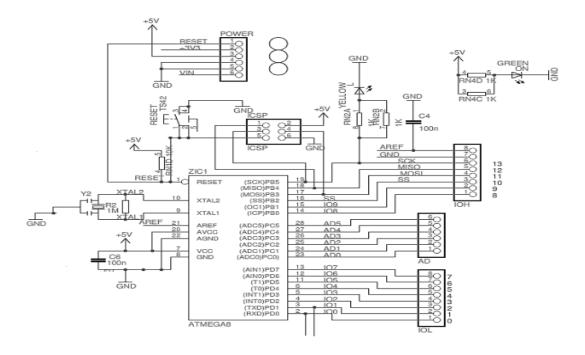


Figure II. 4 : Schéma simplifié de la carte Arduino UNO

Le ATMEL ATMega328 est un microcontrôleur ATMEL de la famille AVR 8bits [25], il se caractérise par [25] :

- **FLASH**: mémoire programme de 32Ko
- **SRAM**: données (volatiles) de 2Ko
- **EEPROM**: données (non volatiles) de 1Ko
- **Digital I/O** (E/S Tout Ou Rien) :3 ports PortB, PortC, PortD (soit 23 broches I/O).
- **Timers/Counters**: Timer0 et Timer2 (comptage 8 bits), Timer1 (comptage 16bits) Chaque timer peut être utilisé pour générer deux signaux PWM. (6 broches OCxA/OCxB).
- **Plusieurs broches multi-fonctions :** certaines broches peuvent avoir plusieurs fonctions différentes choisies par programmation.
- PWM: 6 broches OC0A(PD6), OC0B(PD5), 0C1A(PB1), OC1B(PB3), OC2A(PB3),
 OC2B(PD3)
- Analog to Digital Converter (résolution 10bits): 6 entrées multiplexées ADC0(PC0)
 à ADC5(PC5).
- Gestion bus I2C (TWI TwoWire Interface): le bus est exploité via les broches SDA(PC5)/SCL(PC4).
- **Port série** (**USART**): émission/réception série via les broches TXD(PD1)/RXD(PD0)
- **Comparateur Analogique:** broches AIN0(PD6) et AIN1 (PD7) peut déclencher interruption Watch dog Timer programmable.
- Gestion d'interruptions (24 sources possibles (interruptvectors)) : en résumé
 - o Interruptions liées aux entrées INT0 (PD2) et INT1 (PD3)
 - o Interruptions sur changement d'état des broches PCINT0 à PCINT23
 - o Interruptions liées aux Timers 0, 1 et 2 (plusieurs causes configurables)
 - o Interruption liée au comparateur analogique
 - o Interruption de fin de conversion ADC
 - o Interruptions du port série USART Interruption du bus TWI (I2C).

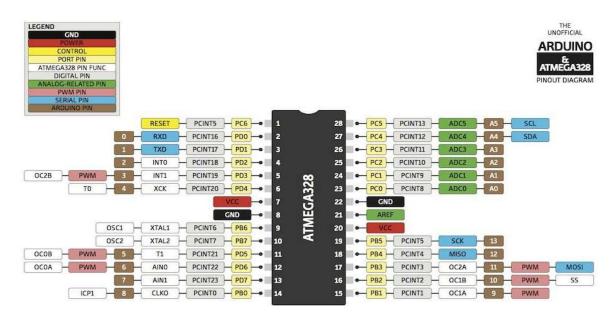


Figure II. 5 : Brochage de Microcontrôleur ATMega328

II. 2. 1. 3. Alimentation de la carte ARDUINO UNO

La carte Arduino UNO peut être alimentée via la connexion USB ou avec une alimentation externe, la source d'alimentation est automatiquement sélectionnée. Une alimentation externe peut provenir soit d'un adaptateur AC-DC ou d'une batterie. L'adaptateur peut être connecté en branchant une prise 2.1mm dans la prise d'alimentation de la carte ou à partir d'une batterie connectée dans le pin (ou broche) GND et Vin (alimentation externe) [26].

- Le processeur peut fonctionner sur une alimentation externe de 6 à 20 V. Cependant, si la tension est inférieure à 7V, le pin 5V peut fournir moins de 5 V et le processeur peut devenir instable.
- Si la tension est supérieure à 12V, le régulateur de tension peut surchauffer et endommager la carte, la plage recommandée est de 7 à 12 V [27].

II. 2. 2. Module RFID

a) Porte clé

Le porte-clés RFID est un produit simple et pratique qui s'adapte à toutes les situations. Cette clé RFID permet un contrôle d'accès fiable et sécuritaire à l'entrée des immeubles, des parkings ou de portes sécurisées grâce au tag RFID [28].

b) Badge RFID

Le badge RFID devient incontournable pour faciliter et sécuriser l'accès aux bâtiments des entreprises. Ces badges RFID sont munis d'une antenne et d'une puce aussi, pour permettre la transmission de données avec un lecteur. Il est réalisé à partir d'un PVC ultra blanc offrant une résistance parfaite lors de manipulations répétées. Le badge RFID est au format : 84 x 56 x 0.76 mm.

c) Le module RC522

Est une interface qui permet l'identification sans contact à partir d'un badge ou une clé RFID. Il est basé sur le circuit intégré Philips RC522. Il utilise la bande 13,56 MHz, la distance de communication peut aller jusqu'à 6cm.

Voltage: 3.3V, courant: 13-25 mA

Fréquence d'utilisation : 13,56 MHz, distance opérationnelle : 0 ~ 60 mm

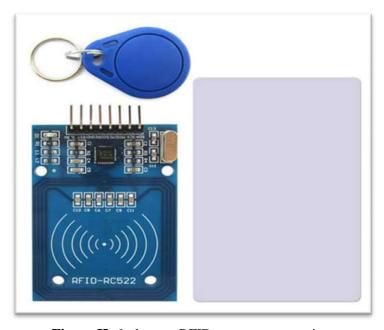


Figure II. 6: lecteur RFID aves ses accessoires

II. 3. Unité de sortie et de communication (Afficheur LCD)

Les afficheurs à cristaux liquides, autrement appelés afficheurs LCD (Liquid Crystal Display), sont des modules compacts intelligents et nécessitent peu de composants externes pour un bon fonctionnement. Ils consomment relativement peu (de 1 à 5 mA), ils sont relativement bons marchés et s'utilisent avec beaucoup de facilité [34].

Plusieurs afficheurs sont disponibles sur le marché et diffèrent les uns des autres, non seulement par leurs dimensions, (de 1 à 4 lignes de 6 à 80 caractères), mais aussi par leurs

caractéristiques techniques et leur tension de service. Certains sont dotés d'un rétro éclairage de l'affichage. Cette fonction fait appel à des LED montées derrière l'écran du module, cependant, cet éclairage est gourmand en intensité (de 80 à 250 mA) [34].



Figure II. 7: Afficheur LCD et accessoires associées

II. 3. 1. Brochage d'un afficheur LCD

Le brochage d'un écran LCD est "normalisé" avec 14 broche (ou 16 si l'écran est rétro éclairé) pour les "petits formats"[35] :

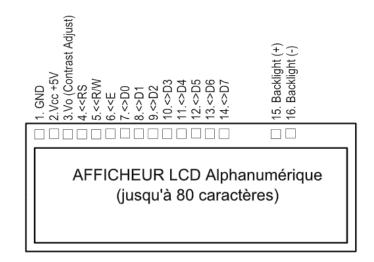


Figure II. 8 : Brochage d'un écran LCD

Broche	Nom	Niveau	Fonction
1	GND	-	Masse
2	V_{CC}	-	Alimentation positive (+5V).
3	Vo	0-5V	Cette tension permet, en la faisant varier entre 0 et +5V, le réglage du contraste de l'afficheur.

Sélection du registre (Registre Select) Grâce à cette broche, l'afficheur est capable de faire la différence entre une commande et une donnée. Un niveau bas indique une commande et un niveau haut indique une donnée. RW Lecture ou écriture (Read/Write) L: Écriture H: Lecture Entrée de validation (Enable) active sur front descendant. Le niveau haut doit être maintenue pendant au moins 450 ns à l'état haut. DO TTL Bus de données bidirectionnel 3 états (haute impédance lorsque E=0) Bus de données bidirectionnel 3 états (haute impédance lorsque E=0) TTL 10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V) Anode rétro éclairage (masse)					
RW TTL Lecture ou écriture (Read/Write) L: Écriture H: Lecture Entrée de validation (Enable) active sur front descendant. Le niveau haut doit être maintenue pendant au moins 450 ns à l'état haut. TTL Bus de données bidirectionnel 3 états (haute impédance lorsque E=0) B D1 TTL 10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL Anode rétro éclairage (+5V)	4	RS	TTL	cette broche, l'afficheur est capable de faire la différence entre une commande et une donnée. Un niveau bas indique une commande et un niveau	
6 E TTL descendant. Le niveau haut doit être maintenue pendant au moins 450 ns à l'état haut. 7 D0 TTL Bus de données bidirectionnel 3 états (haute impédance lorsque E=0) 8 D1 TTL 9 D2 TTL 10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	5	RW	TTL	Lecture ou écriture (Read/Write) L : Écriture	
7 D0 TTL (haute impédance lorsque E=0) 8 D1 TTL 9 D2 TTL 10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	6	Е	TTL	descendant. Le niveau haut doit être maintenue	
9 D2 TTL 10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	7	D0	TTL		
10 D3 TTL 11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	8	D1	TTL		
11 D4 TTL 12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	9	D2	TTL		
12 D5 TTL 13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	10	D3	TTL		
13 D6 TTL 14 D7 TTL 15 A - Anode rétro éclairage (+5V)	11	D4	TTL		
14 D7 TTL 15 A - Anode rétro éclairage (+5V)	12	D5	TTL		
15 A - Anode rétro éclairage (+5V)	13	D6	TTL		
	14	D7	TTL		
16 K - Cathode rétro éclairage (masse)	15	A	-	Anode rétro éclairage (+5V)	
	16	K	-	Cathode rétro éclairage (masse)	

Tableau II. 2 : Rôle et nom de chaque broche d'un afficheur LCD

Tout projet qui nécessite tant de convivialité ou de contrôle pour l'utilisateur doit comporter un afficheur. En effet, celui-ci permet de manière très rapide de révéler n'importe quelle information qui pourrait être utile au programmeur ou à l'usager.

II. 3. 2. Principe de fonctionnement d'un écran LCD

L'afficheur LCD est constitué de deux polariseurs dont les directions de polarisation forment un angle de 90°, de chaque côté d'un sandwich formé de deux plaques de verre enserrant des cristaux liquides. À chacune des interfaces avec les cristaux liquides, une couche de polymère, généralement un polyamide, rainurée assure l'ancrage des molécules au repos [36].

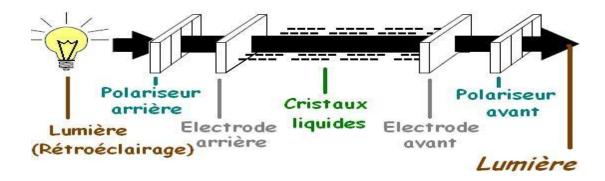


Figure II. 9 : Principe de fonctionnement d'un écran LCD

II. 4. Unité d'entrée

II. 4. 1. Clavier matriciel

Le clavier numérique est plus aisé et plus pratique à utiliser, il présente la communication Homme-Machine [38].

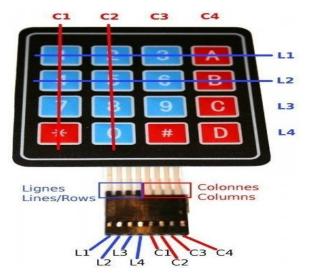


Figure II. 10: Clavier matriciel

Le code étant numérique, donc il nous suffit de choisir un clavier douze touches dont il y'a deux boutons spéciaux, un capable de changer facilement le mot de passe et l'autre efface l'écran en cas d'erreur de frappe [38].

Exemple : On introduisant le code d'accès qui est par défaut 1234, suivant « * », la LED jaune s'allume signifiant l'activation du relais.

Si on introduit un code erroné plus de trois fois, l'ADUINO génère un signal pour l'activation d'une alarme par exemple.

Si nous voudrions changer le code d'accès, nous aurons obligé à suivre les étapes suivantes :

appuyer sur la touche «# » : l'usager entre en mode de programmation.

- entrer l'ancien code.
- appuyer sur « # ».
- entrer le nouveau code d'accès désirer.
- appuyer sur « * » [39].

II. 5. Composants auxiliaires

II. 5. 1. Buzzer

Un Buzzer est un élément électromécanique ou électronique qui produit un son quand on lui applique une tension. Certains nécessitent une tension continue (Buzzers électromécaniques), d'autres nécessitent une tension alternative (transducteurs piézo-électrique) [40].





Figure II. 11: Buzzer 1. Electromécaniques

2. Piézo-électrique

Le son émet est simplement une vague de pression d'air variable. Ces ondes de pression provoquent une vibration de la membrane mince dans l'oreille et le cerveau interprète ces vibrations comme un son. Une échelle de décibels (dB) est utilisée pour décrire le niveau de pression acoustique [41].

II. 5. 2. Servomoteur

Le servomoteur intègre un système électronique qui converti un signal numérique en un angle qui sera reproduit grâce au moteur électrique à courant continu présent dans le servomoteur. Le servomoteur est alimenté avec 3 fils : une entrée 5V, une masse et une entrée d'impulsion (la commande du servomoteur). C'est dans cette entrée d'impulsion qu'est envoyé le signal numérique modulé en impulsions. Ces impulsions sont des créneaux à rapport cyclique variable et ce signal numérique va alors contrôler le servomoteur en position.



Figure II.12: Servomoteur

Dans notre projet, le choix du servomoteur a été fait selon les besoins et les fonctions qu'il doit accomplir. Il s'agit d'un servomoteur commandant la rotation horizontale à un angle de 180° [28].

II. 6. Conclusion

Dans le présent chapitre nous avons présenté la partie théorique des différents modules constituant notre carte électronique pour un système de contrôle d'accès.

La première partie du présent chapitre a été consacré pour la présentation des caractéristiques techniques et le schéma simplifie de la carte Arduino. La deuxième partie de ce chapitre, présente l'unité d'entré via carte RFID avec les différents protocoles de communications entre l'unité de commande et les périphériques d'entrées et de sortie ainsi le clavier matriciel. Dans la troisième partie nous avons présenté l'unité de sortie et de communication (Afficheur LCD). La dernière partie présente les composants auxiliaires tels que l'horloge et le Buzzer et le servomoteur nécessaire au bon fonctionnement du montage.

Chapitre III

Réalisation d'un système de contrôle d'accès sécurisé

Chapitre III: Réalisation d'un système de contrôle d'accès sécurisé

III. 1. Introduction

Le bon déroulement de toute réalisation nécessite une étude théorique, alors nous avons présentée dans le chapitre les différentes étapes de la conception de notre projet et comment réaliser un système de contrôle d'accès sécurisé à base de la technologie RFID gérer par une carte Arduino. Parmi les applications de ce système, nous avons choisi la commande d'ouverture automatique d'une porte ou d'une barrière d'un parking par exemple on utilisant un servomoteur.

III. 2. Partie simulation

III.2. 1. Organigramme de fonctionnement

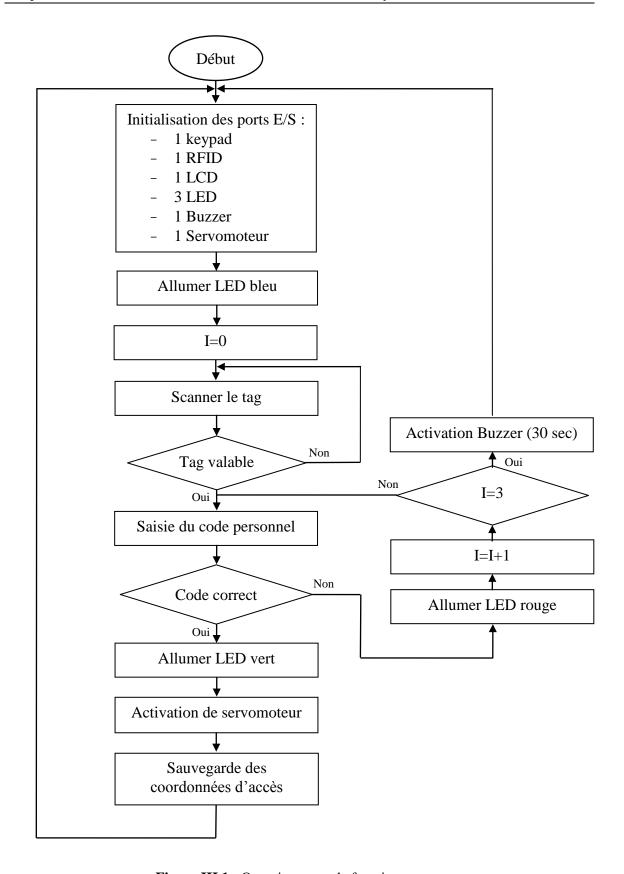


Figure III.1 : Organigramme de fonctionnement

III.2. 2. Schéma synoptique du système

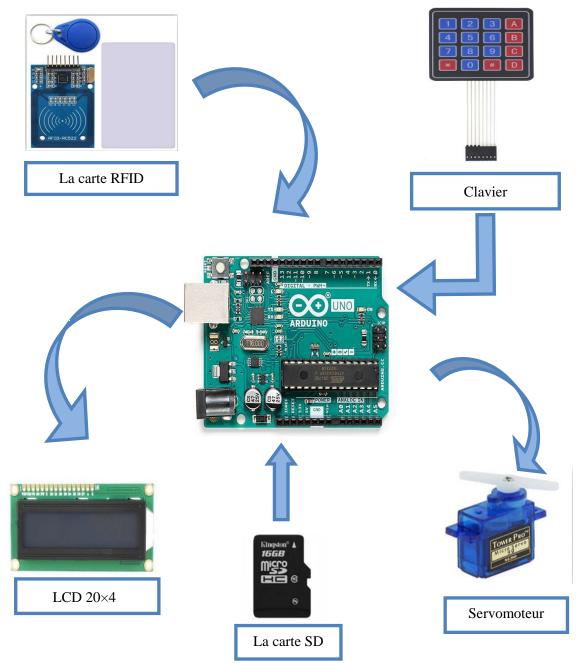


Figure III. 2 : Schéma synoptique du système

III. 3. Câblage de montage

III. 3. 1. Câblage de LED

Une fois que notre montage est raccordé, on va mettre en place les témoins lumineux (LED verte et LED rouge). On câble l'anode du LED verte en série avec une résistance de protection sur la sortie numérique de l'Arduino, de même pour la LED rouge. La LED verte va s'allumer si la carte autorisée est passe devant le lecteur RFID et la LED rouge reste allumer si la carte non autorisée passe devant le lecteur.

Pour ce faire nous allons donc procéder ainsi : Arduino → LED

- 1. LED verte
- 2. LED rouge

Le montage de base d'une LED est ressemblé à ça :

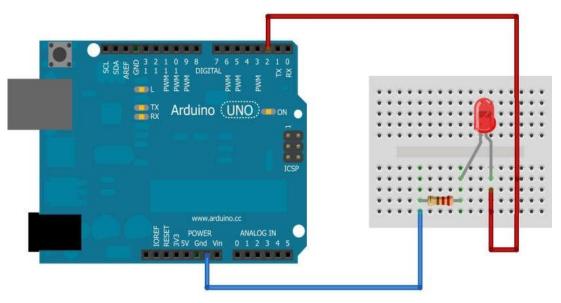
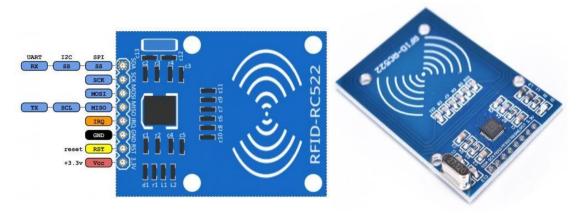


Figure III. 3: Montage carte Arduino +LED

III. 3. 2. Câblage module RFID (RC-522)

Notre montage devrait donc ressembler à ça :

Туре	Symbole	Description
	3.3V	VCC
Les broches	RST	Reset
Du MFRC522	GND	Ground
	IRQ	Interrupt request
	MISO	Interface SPI
	MOSI	Interface SPI
	SCK	Interface SPI
	SS	Sélection esclave



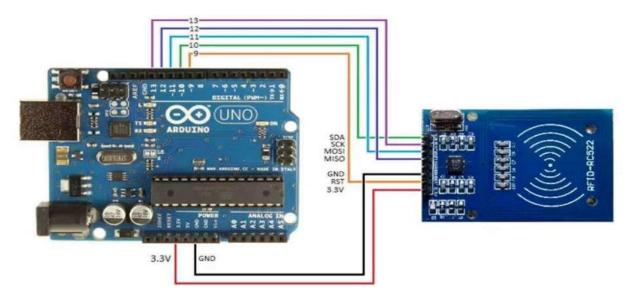


Figure III. 4: Montage carte Arduino + lecteur RFID

Nous allons donc raccorder comme ceci : Arduino →RC-522

- 3.3v sur 3.3v
- GND sur gnd
- SDA sur D10
- SCK sur D13
- MOSI sur D11
- MISO sur D12
- RST sur D9

III. 3. 3. Câblage d'un afficheur LCD

L'afficheur LCD utilisé est un écran permettant l'affichage de 16×2 caractères, c'est-àdire deux lignes de 16 caractères.

Le montage que nous allons réaliser va connecter l'afficheur LCD à l'Arduino, et ajouter un potentiomètre pour ajuster le contraste. Le transfert des données sous forme de bits est pris en compte par la bibliothèque 'LiquidCrystal'.

- La broche V_{SS} est reliée à la masse (GND).
- La broche V_{DD} est reliée à l'alimentation 5 V.
- R_S est reliée au port digital 12.
- RW est reliée à la masse, une façon de lui donner une valeur basse pour passer en mode

écriture.

- E est relié au port digital 11.
- V0 est reliée à la broche de données du potentiomètre (au centre).
- La broche à gauche derrière la broche seule sur sa rangée (3) du potentiomètre est reliée à 5 V.
- La broche à droite à la masse.
- Les broches D4 à D7 du LCD sont reliées aux ports digitaux 4 à 7 de l'Arduino.

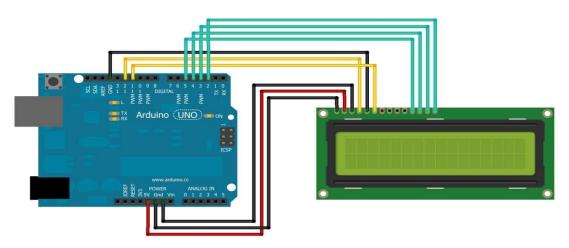


Figure III.5: Montage carte Arduino + afficheur

III. 3. 4. Câblage de servomoteur

Les servomoteurs sont des moteurs un peu particuliers, qui peuvent tourner avec une liberté d'environ 180° et garder de manière relativement précise l'angle de rotation que l'on souhaite obtenir.

Nous avons utilisé une broche qui est une entrée numérique afin de commander notre moteur alimenté à partir de notre carte Arduino (5 V).

Dans notre programme nous utilisons la librairie SERVO qui regroupe un grand nombre de fonctions permettant de contrôler le servomoteur.

La carte Arduino a été liée au servomoteur en plus d'un module RFID selon le schéma ci-dessous :

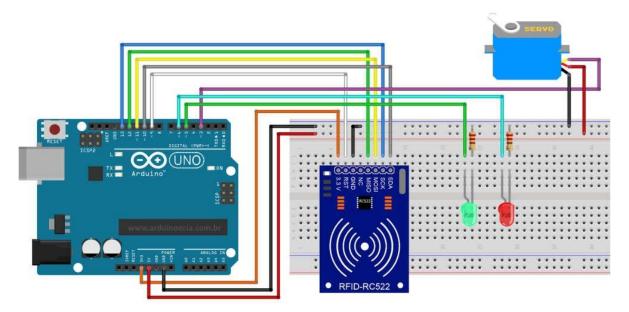


Figure III.6: Montage carte Arduino +lecteur RFID + servomoteur

III. 3. 5. Logiciel (IDE Arduino)



Figure III.7: Logo Arduino

L'environnement de programmation Arduino (IDE en anglais) est une application écrite en Java. L'IDE permet d'écrire, de modifier un programme et de le convertir en une série d'instructions compréhensibles pour la carte. Le logiciel va nous permettre de programmer la carte Arduino, il nous offre une multitude de fonctionnalités.

La structure des programmes Arduino est un peu particulier, en apparence, des structures habituelles du langage C. La syntaxe est la même qu'en langage C.

Au début du programme, la déclaration des librairies utilisée par le programme à compiler avec le programme.

- **Nouveau** : pour créer un nouveau programme (sketch).
- Ouvrir : ouvrir un programme existant. Le menu n'est pas déroulant à cause d'un bug...pour obtenir un menu déroulant passer par file/open
- Enregistrer : sauvegarde le programme, si vous voulez le sauvegarder sous un autre

nom, passer par file/Save as.

- Moniteur série : pour ouvrir la fenêtre qui permet de visualiser les données transmise par le port série de l'Arduino.
- Le programme est lu par le microcontrôleur de haut vers le bas.
- Une variable doit être déclarée avant d'être utilisée par une fonction.

La structure minimale est constituée :

- En tête : déclaration des variables, des constantes, indication de l'utilisation de bibliothèques etc...
- un setup (ou initialisation) cette partie n'est lue qu'une seule fois, elle comprend les fonctions qui doivent être réalisées au démarrage (utilisation des broches en entrées ou en sortie)

Une loop (boucle) : cette partie est lue en boucle, c'est ici que les fonctions sont réalisées.

Figure III.8: Logiciel (IDE Arduino)

III. 3. 6. La macro PLX-DAQ

PLX-DAQ est une macro pour Excel mise au point par la société Parallax pour permettre aux microcontrôleurs qu'elle commercialise d'envoyer des données vers Excel. C'est gratuit, et ça fonctionne avec n'importe quel microcontrôleur capable de communication série, ce qui inclut bien sûr l'Arduino.

Avec PLX-DAQ, nous pouvons envoyer les données en temps réel collectées par Arduino dans Excel, où il est beaucoup plus facile de traiter les données.

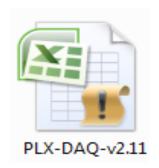


Figure III.9: logo PLX-DAQ-v2.11 Excel

Remarque : Par défaut, Excel est plutôt paranoïaque en ce qui concerne les macros : en mode "Niveau de sécurité élevé", il refuse de les exécuter, par crainte qu'elles contiennent des virus. Pour vérifier le niveau de sécurité de votre exemplaire d'Excel (et pour le modifier s'il n'est pas adéquat), choisissez "Options" dans le menu "Outils".

a) Partie Arduino

Dans la fonction de configuration du sketch Arduino, incluez ces codes :

- Serial.begin (9600);
- Serial.println("CLEARDATA");
- Serial.println("LABEL,Acolumn,Bcolumn,...");
- Serial.println("RESETTIMER");

Il s'agit de directives de contrôle pour le PLX-DAQ.

- CLEARDATA efface les données précédentes dans la colonne,
- la directive LABEL spécifie le nom des colonnes,
- RESETTIMER réinitialise le timer interne.

Dans la fonction loop(), incluez d'abord cette directive de contrôle.

 Serial.print("DATA,TIME,TIMER,"): DATA spécifie que le reste de la sortie série sera étiqueté comme données et enregistré dans la colonne. Les deux premiers paramètres sont TIME qui spécifie l'heure actuelle et TIMER qui enregistre le temps écoulé depuis son démarrage.

Ensuite, il suffit d'imprimer les valeurs qui ont dû être imprimées. N'oubliez pas de commencer une nouvelle ligne et d'inclure un délai à la fin :

- Serial.println();
- delay(100);

b) Partie Excel

Lancer le fichier Excel ; cliquez sur OK dans la boîte de dialogue. Celle-ci apparaîtra alors :

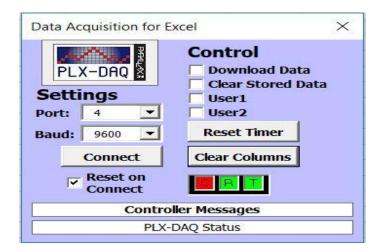


Figure III.10 : Acquisition des données à partir de fichier Excel

Choisissez le bon port dans Arduino et le bon baud, cliquez sur "connecter", et les données devraient apparaître dans le fichier Excel. (N'oubliez pas de télécharger le code Arduino)

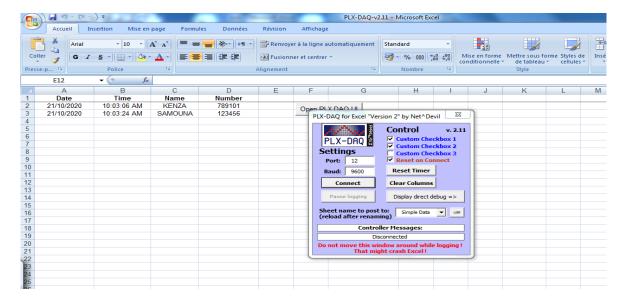


Figure III.11: Exemple de lecture de fichier Excel

Le fichier Excel comporte trois onglets, il s'agit de données simples, de données simples avec tracés et d'un graphique à barres interactif. Le script s'exécutera sur la première position de l'onglet ; déplacez les onglets en conséquence pour répondre aux différents besoins.

III. 3. 7. Montage à ISIS Proteus

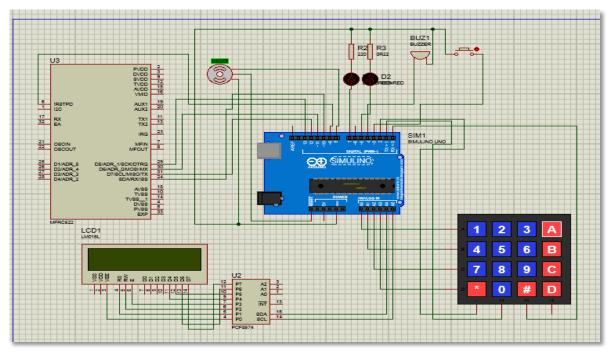


Figure III. 12 : Montage de simulation de système de contrôle d'accès sécurisé à base de la technologie RFID

III. 3. 8. Le montage global

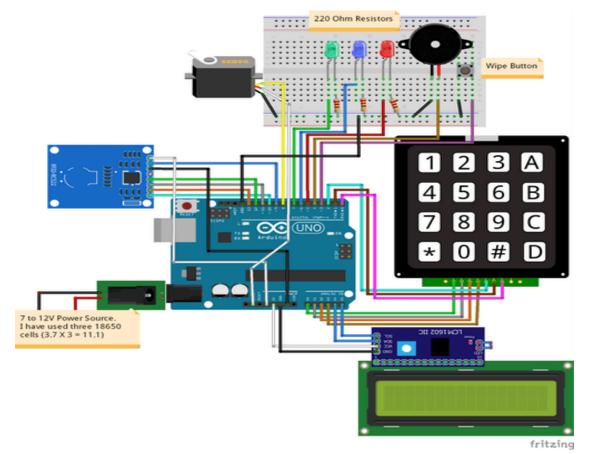


Figure III .13: Le schéma général (Fritzing)

III. 4. La partie expérimentale

Le montage expérimental est le suivant :

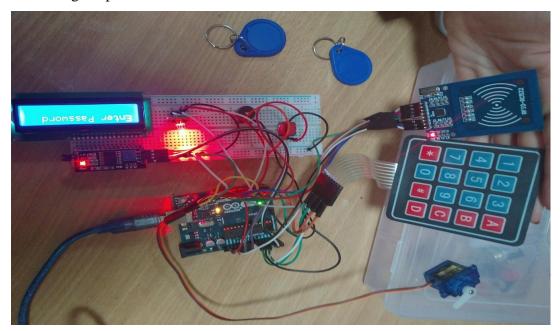


Figure III.14: Montage expérimental

III. 5. Conclusion

Dans ce dernier chapitre on a présenté les étapes de création de notre projet qui consiste à l'étude et réalisation d'un système de contrôle d'accès sécurisé avec la technologie RFID. Nous avons commencé notre étude par une simulation par le logiciel ISIS de Labcenter Electronics, on a projeté de la lumière sur les différentes étapes de la réalisation de notre montage y compris le câblage. A la fin, nous avons réalisé notre projet à base d'une carte Arduino connecter au module RFID, utilisant des différents tags (autorisées et non autorisées) nous avons testé le bon fonctionnement de notre montage par le biais d'un affichage LCD et sauvegarde des données sur un fichier Excel. A noter, nous avons ajouté d'autres témoins de bon fonctionnement tels que les LED et un Buzer.

Notre contribution réside dans l'ajout d'un clavier matriciel pour sécuriser en plus notre système d'accès car le tag RFID peut être perdu et n'importe quelle individu peut être l'utiliser.

Conclusion générale

Conclusion générale

En conclusion, l'objectif de mettre en place d'un système d'accès sécurisé basé sur la technologie RFID afin de gérer l'ouverture d'une porte ou d'une barrière dans un parking publique a été atteint avec succès. En termes de performance et d'efficacité, ce projet permet de fourni une méthode pratique de marquage des présences des individus par rapport à la méthode traditionnelle, c'est-à-dire la présence manuelle sur papier. On utilisant des bases de données en temps réel, ces derniers sont mieux organisés et mieux exploiter en terme de sondage, sécurité, calcul divers. Ce système est également convivial car la manipulation et la récupération des données peuvent se faire via des interfaces physiques faciles à utiliser. De plus, ce système basé sur la technologie RFID permet d'améliorer plusieurs secteurs économiques on réduisant le coût et faciliter les traitements de gestion des stocks, l'expédition et l'identification des produits dans les grands magasins.

Egalement, on peut profiter de notre projet dans l'établissement universitaire où l'enseignant ne perd plus de temps pour comptabiliser la présence de ses étudiants.

•

Bibliographie

- [1]. https://www.horloges-huchez.fr/blog/tout-savoir-sur-lepointage consulté le 27/05/2020
- [2]. https://www.horloges-huchez.fr/blog/5-avantages-le contrôle d'accès-horaire- entreprise consulté le 27/05/2020
- [3]. https://www.secu-mag.com.tn/articles/systemes-de-pointage.html consulté le 28/05/2020
- [4]. https://www.futura-sciences.com/fr/definition/t/medecine-2/d/empreintes-digitales_3302 consulté le 28/05/2020
- [5]. https://fingerchip.pagespersoorange.fr/biometrics/types/fingerprint_sensors_physics.htm consulté le 28/05/2020
- [6]. https://www.horloges-huchez.fr/badgeuse consulté le 28/05/2020
- [7]. Ben Hamed Amina et Medjda Omar, 'Reconnaissance des empreintes digital', mémoire de fin d'étude pour l'obtention du diplôme master en informatique 17 juillet 2015.
- [8]. Andrey Murhula, Conception et mise en place d'une plateforme de Sécurisation par Synthèse et reconnaissance biométrique. Documents de Traffic, Polytechnique Initelematique_Burundi Ingénieur Civil en Informatique et télécommunications 2015.
- [9]. https://contrat-de-travail.ooreka.fr/astuce/voir/753019/le contrôle d'accès-biométrique 28/05/2020
- [10]. Perret E, Hamdi M, Vena A,Garet F, Bernier M, Duvillaret L, Tedjinis,-RF and THz Identification Using a new Generation of Chipless RFID Tags. Radio engineering, 2011
- [11]. https://blog.atlas RFID store.com/active-RFID-vs-passive-RFID, consulté le 10/09/2020
- [12]. https://www.atlas RFID store.com/active-RFID/consulté le 10/09/2020
- [13]. https://www.transplanet.fr/biometrie/lecteur_d_empreintes_digitales.html consulté le 11/09/2020
- [14]. katamba, paulini lunga, 'technologie RFID (radio frequency identificatio)' : Concept set stratégie de mise en œuvre'. Université Laval, 2007.
- [15]. Soulami Nouha, Touzani Zineb, 'Conception et développement d'un Système de pointage bassé sur la technologie RFID', Université Sidi Mohammed Ben Abdellah', soutenu le 16 juin 2015
- [16]. Capteurs sans fil basés sur les tags RFID UHF Développement des Nguyen Son Dat 2013 passifs pour la d'détection de la qualité des aliments
- [17]. Caractéristiques des tags RFID Tania martin le b.a.-ba de la RFID origines, technologie et applications publication périodique de smals janvier 2014
- [18]. Antti Ruhanen, Marko Hanhi korpi, Fabrizio Bertuccelli, Annamaria Colonna, Westy Malik, Damith Ranasinghe, Tomas Sánchez López, Na Yan et Matti Tavilampi. 'Sensor-Enabled RFID tag handbook. Building Radio frequency IDentification for the Global Environment Project.2008

- [19]. NORTON, H. <u>Transducer fundamentals</u>. In <u>Handbook of Transducers</u>. <u>Englewood Cliffs NJ</u>: Prentice Hall, ch. 2.1989.
- [20]. HELMUS M ,OFFERGELD B, l'identification par radiofréquence ouvre de nouvelles possibilités à la prévention. KANBrief du 03/2007.
- [21]. https://www.bgi-cartes.fr/applications-domaines-cartes-puces13/10/2020
- [22]. Anes Douidi et Chikh Oussama, 'Conception et simulation de tags RFID' diplôme MASTER . Spécialité: réseau et télecommunication, Faculté de technologie, Université ABoubakr belkaid, Telemcen. 2018
- [23]. http://www.techmania.fr/arduino/Decouverte_arduino.pdf Consulté le 22/09/2020
- [24]. http://perso-laris.univ-angers.fr/~cottenceau/ArduinoCottenceau1112.pdf, Consulté le 22/09/2020
- [25]. http://perso-laris.univ-angers.fr/~cottenceau/ArduinoCottenceau1112.pdf, Consulté le 22/09/2020
- [26]. KRAMA A., GOUGUI A., 2015. «Etude et réalisation d'une carte de contrôle par Arduino via le système Androide », mémoire Master Académique, Université KasdiMerbah Ouargla.
- [27]. Nicolas G., Goeffrey L., 2015. Arduino Apprendre à développer pour créer des objets intelligents
- [28]. Mémoire du projet de fin d'études Pour l'obtention de diplôme Master Université Djilali Bounaama Khemis Miliana En Télécommunication, 'Conception et implémentation du système Radio Frequency Identification à l'aide d'une carte Arduino et lecteur RFID'. Année universitaire 2016-2017
- [29]. https://www.editionseni.fr/open/mediabook.aspx?idR=c642d6d1 e5b48f4a4be571. 215281f consulté le 06/10/2020
- [30]. https://openclassrooms.com/fr/courses/3290206-perfectionnez-vous-dans-la-programmation-arduino/3370761-decouvrez-le-shield-ethernet-et-le-lecteur-de-carte-sd . consulté le 10/10/2020
- [31]. https://www.w3schools.com/html/html_editors.asp consulté le 10/10/2020
- [32]. https://github.com/CisecoPlc/Arduino-W5100-W5200/tree/master/Ethernet, consulté le 10/10/2020
- [33]. https://zestedesavoir.com/tutoriels/686/arduino-premiers-pas-en-informatique-embarquee/1213_internet-of-things-arduino-sur-internet/4846_decouverte-de-lethernet-sur-arduino, consulté le 19/10/2020
- [34]. https://www.aurel32.net/elec/lcd.php Consulté le20/10/2020
- [35]. http://dessoudeurs-ex.lebonforum.com/t17-initiation-pic-afficheur-lcd], consulté le20/10/2020
- [36]. Sayah_manal, système de pointage Empreinte digital. Mémoire de fin d'étude pour l'obtention du diplôme Master en Electronique Système embarqué. 20-Jun-2019
- [37]. https://fr.scribd.com/doc/35887890/Les-Afficheurs-LCD Consulté le 20/10/2020
- [38]. https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&u act=8&ved=0ahUKEwig35jD393SAhXGPBQKHQtQDh8QFgg8MAk&url=http%3A%1.docx

&usg=AFQjCNGCF5LvhQW8C5RzYPyvOuWsIrexiQ&bvm=bv 1.docx&usg=AFQjCNGCF5LvhQW8C5RzYPyvOuWsIrexiQ &bvm=bv. 149760088,d D24, consulté le 20/10/2020

- [39]. http://docslide.fr/documents/serrure-codee-par-un-pic-16f628.html, consulté le 20/10/2020
- [40]. https://www.sonelec-musique.com/electronique_theorie_buzzers.html, consulté le 20/10/2020
- [41]. http://docslide.fr/documents/serrure-codee-par-un-pic-16f628.html, consulté le 20/10/2020

ملخص

في هذا المشروع قمنا بإنشاء نظام تحكم آمن في الولوج للمباني والحضائر العمومية يعتمد على تقنية RFID باستخدام المعالج Arduino حيث يتعين على المستخدم تمرير البطاقة الصحيحة أولاً وإدخال كلمة المرور الخاصة به. كما أضفنا للنظام مؤشرات ضوئية وصوتية تمكن المستعمل من معرفة صحة أوخطأ ما يقوم به بالإضافة لشاشة صغيرة LCD تضمن التعامل المباشر مع النظام وفق الخيارات المتاحة.

كما يسمح النظام المقترح بتخزين قائمة الأشخاص الذي استعملوه بكل التفاصيل من حيث الوقت وتاريخ الدخول. هذا النموذج يمكن استعماله لأغراض تجارية في المؤسسات الاقتصادية وكذلك على مستوى الإدارات والمؤسسات التعليمية.

Résumé

Dans ce projet, nous avons réalisé un système de contrôle d'accès sécurisé basé sur la technologie RFID et gérer par la carte Arduino afin de commander une porte ou une barrière dans un parking publique dans lequel l'utilisateur devra d'abord scanner la bonne étiquette et ensuite il devra entrer son mot de passe. Nous avons également ajouté d'autres témoins tels que les LED et un Buzzer afin que l'utilisateur sait gérer son système, en plus un afficheur LCD qui garantit l'interaction homme-machine.

Le système proposé permet de sauvegarder tous les détails et informations des gens qu'ils ont utilisées dans le but d'exploiter la base de données. On peut également utiliser ce système dans des magasins commerciaux ou dans des administration et établissements d'enseignement.

Abstract

In this project, we have realized a secure access control system based on RFID technology and managed by the Arduino board in order to control door or barrier in a public parking in which the user will first have to scan the correct tag and then he will have to enter his password. We have also added other indicators such as LEDs and a Buzzer so that the user can manage their system, in addition an LCD display that guarantees human-machine interaction.

The proposed system saves all the details and information of the people they have used in order to operate the database. This system can also be used in commercial stores or in administration and educational establishments.