République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE**T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDE DE MASTER ACADEMIQUE

Domaine : Mathématiques et Informatique
Filière : Informatique

Spécialité : **Réseaux, Mobilités et Systèmes Embarqués**

Présenté par

OUKIL Kahina

ZERBOUT Ania

Thème

Contrôle d'accès à base d'empreinte digitale

Mémoire soutenu publiquement le 05/09/2019 devant le jury composé de :

Présidente : Mme OUKFIF karima

Examinateur : Mme Khiali linda

Encadreur : Mr DAOUI Mehammed

Dédicaces

A la mémoire de mon grand père

Puisse Dieu l'accueillir dans son infinie Miséricorde

Je dédie ce mémoire à :

Mes chers parents, que nulle dédicace ne puisse exprimer mes sincères sentiments pour leur patience illimitée, leur encouragement, leur aide, en témoignage de mon profond amour et respect pour leur grand sacrifice.

Mes modèles et exemples, mon sang, Mon cher frère : Karim, Ma chère sœur Samia et son Mari Karim pour leur grand amour et leur soutient qu'ils trouvent ici l'expression de ma haute gratitude.

Mes grands-parents qui ont toujours été présent pour les bons conseils, leur affection et leur soutient m'ont été d'un grand secours au cours de ma vie.

Tous les membres de ma famille petits et grands veuillez trouver dans ce modeste travail expression de mon affection.

A ma chère binôme ***Ania***

A tous mes amis (es) et camarades.

A mon promoteur Mr ***DAOUI Mehammed*** *dont le professionnalisme n'a d'égal.*

-Kahina-

Dédicaces

A la mémoire de mes grands-parents, mon oncle

Puisse Dieu les accueillir dans son infinie Miséricorde

Je dédie ce mémoire à :

Mes chers parents, que nulle dédicace ne puisse exprimer mes sincères sentiments pour leur patience illimitée, leur encouragement, leur aide, en témoignage de mon profond amour et respect pour leur grand sacrifice.

Mes modèles et exemples, mon sang, Mes chers frères : Nounou et Moh-rabeh pour leur grand amour et leur soutient qu'ils trouvent ici l'expression de ma haute gratitude.

Mes grands-mères qui ont toujours été présentes pour les bons conseils, leur affection et leur soutient m'ont été d'un grand secours au cours de ma vie.

Tous les membres de ma famille petits et grands veuillez trouver dans ce modeste travail l'expression de mon affection.

A ma chère binôme ***Kahina***

A tous mes amis (es) et camarades.

A mon promoteur Mr ***DAOUI Mehammed*** *dont le professionnalisme n'a d'égal.*

-Ania-

Remerciement

Tout d'abord, nous tenons à remercier le ***Bon Dieu*** *tout puissant pour nous avoir donné patience, courage, volonté et l'intelligence nécessaire pour accomplir ce modeste travail et nous avoir permis de le mener à bien.*

Nous tenons à exprimer notre immense gratitude à l'encadreur de ce travail, Monsieur ***DAOUI Mehammed****, Professeur à l'université Mouloud Mammeri Tizi Ouzou, qui est l'exemple de chercheur passionné que l'on souhaite devenir un jour.*

Nos remerciements vont à lui, pour avoir guidé nos premiers pas dans la recherche et pour nous avoir encadrés.

Nous le remercions vivement pour la confiance qu'il nous a accordés, ses conseils et remarques constructives qui nous ont permis d'améliorer la qualité de notre travail.

Nous ne saurons jamais assez remercier Monsieur ***RAVI*** *pour le temps qu'il nous a consacré, son aide, ses conseils, et ses orientations. Qu'il trouve ici l'expression de notre profonde gratitude.*

Nous adressons nos plus sincères remerciement à Madame ***Oukfif Karima*** *et Madame* ***Khiali Linda*** *pour l'intérêt qu'ils ont porté à notre travail en examinant ce mémoire et en participant à ce jury.*

Table des Figures :

Table des matières

Chapitre V : **Mise en œuvre**

Table des figures :

Introduction générale

Le besoin en confort et en sécurité de nos sociétés modernes devient de plus en plus important, Les outils classiques tel que les mots de passes et les badges ne suffisent plus pour répondre à ces besoins car l'utilisation d'un mot de passe nécessite sa mémorisation et le fait d'en avoir plusieurs rendent la tâche plus difficile, le noter engendre le risque de perte ou de vol. De même, l'utilisation de cartes magnétiques ou de badges n'échappe pas au risque de vol par des imposteurs qui sont capables de falsifier leur identité. Toutes ces difficultés ont donné naissance à l'idée d'utiliser des caractéristiques biométriques comme moyen de contrôle d'identité.

La biométrie consiste à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres. En d'autres termes, c'est une approche permettant de déterminer l'identité d'un individu par la reconnaissance automatique de certaines de ses caractéristiques physiques ou comportementales. Elle facilite l'accès pour les usagers tout en garantissant un niveau de sécurité élevé, elle pallie aux risques de vol des cartes d'accès ou d'oubli des mots de passe.

Il existe plusieurs caractéristiques physiques et comportementales uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, citons : L'empreinte digitale, La dynamique des signatures, l'iris, la rétine, la reconnaissance vocale et celle du visage.

Dans ce cadre, notre projet de fin d'études a comme objectif de développer un système de contrôle d'accès reposant sur l'une des techniques biométriques les plus utilisées, qui est la reconnaissance d'empreinte digitale, Elle est utilisée depuis un siècle pour l'identification criminelle. Elle correspond à l'essentiel du marché actuel et son utilisation sera sans doute amenée à se développer. Cette dernière possède un taux de fiabilité suffisant pour permettre d'identifier les individus dans de grandes bases de données.

Nous allons donc développer un système de contrôle pour un accès (la porte d'entrée d'une maison, un bureau, un laboratoire, une entreprise, ...etc). Ce système identifie les personnes autorisées à accéder par leurs empreintes digitales enregistrées au préalable. Quand une personne souhaite accéder, elle place son doigt dans le lecteur d'empreinte. Une fois l'empreinte lue, le système vérifie les autorisations et déclenche le signal d'ouverture qui actionne une gâchette électrique dans le cas où la personne est autorisée. Le système permet aussi d'enregistrer les dates et heures d'accès à des fins de traçabilité. Il dispose aussi de mécanismes de communication divers notamment l'accès par réseau wifi à un serveur web pour l'enregistrement des accès et un accès filaire via le bus I2C pour faciliter son intégration dans une Smart home.

Afin de bien mener à terme notre projet et de donner une démarche compréhensible, nous avons structuré le présent mémoire de la manière suivante :

Après une brève introduction, dans laquelle nous cernons la thématique, de manière globale, le but du projet et les solutions envisageables, nous entamons notre mémoire par le premier chapitre qui est consacré à la présentation des notions générales de la biométrie.

Nous enchainons par le deuxième chapitre qui donne un aperçu sur la technique de biométrie utilisée dans notre projet qui est l'empreinte digitale.

Le troisième chapitre est dédié à la présentation des systèmes embarqués et leurs applications. En particulier, nous avons présenté en détail un protocole de communication pour les smart home qui est le protocole I2C.

Enfin, les deux derniers chapitres ont été consacré à la partie conception et réalisation pratique de notre travail. Il présente la démarche suivie pour réaliser ce système, ainsi que la présentation du prototype final obtenu.

Chapitre I

Généralités sur la biométrie

I.1 Introduction

De nos jours, on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrarier cette tendance : le contrôle d'accès aux ordinateurs, l'e-commerce, les opérations bancaires basées sur l'identification du demandeur, etc. Cette insécurité est due à l'usage des méthodes classiques d'identification qui posent de gros problèmes de fiabilité comme : le mot de passe qui peut être oublié ou décrypté via des logiciels spécifiques. Afin de répondre à ces besoins liés à la sécurité, la biométrie se présente comme une technologie potentiellement puissante.

Au niveau de ce chapitre, nous allons présenter les notions fondamentales de la biométrie. Nous allons étudier dans un premier lieu sa définition puis son historique, ses différents domaines d'application, ses catégories technologiques ainsi que ses techniques. Nous aborderons par la suite l'état du marché et ses parts par technologies.

I.2 Définition de la biométrie [1]

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques(humaine) préalablement enregistrée : physiologique, comportementale, biologique, ...etc.

Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

I.3 Les applications de la biométrie [2]

Le champ d'application de la biométrie couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes.

Aujourd'hui, les principales applications sont la production de titre d'identité, le contrôle d'accès à des sites sensibles, le contrôle des frontières, l'accès aux réseaux, le paiement électronique, et la protection des données privées, etc…. De nouvelles applications vont certainement voir rapidement le jour.

Les secteurs en pleine progression dans ce domaine sont :

• Le contrôle d'accès physique aux locaux : salle informatique, site sensible (bases militaires, service de recherche…).

• Le contrôle d'accès logiques aux systèmes d'informations : lancement du système d'exploitation, accès au réseau informatique, commerce électronique, transaction

(financière pour les banques, données des entreprises), tous les logiciels utilisant un mot de passe.

• Contrôle d'utilisation d'équipements de communication : terminaux d'accès à internet, téléphones portables.

• Contrôle de machines et équipement divers : coffre-fort avec serrure électronique, distributeur automatique de billets, carte de fidélité, voiture (anti-démarrage) …

I.4 Les catégories technologiques de la biométrie [3]

Il existe trois grandes catégories de biométrie : la biométrie morphologique, la biométrie comportementale et la biométrie basée sur l'étude des traces biologiques.

I.4.1 La biométrie morphologique

Appelée aussi biométrie physiologique, elle se base sur les traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris.

I.4.2 La biométrie comportementale

Elle est basée sur l'analyse de certains comportements d'une personne comme le tracé de sa signature (inclinaison et vitesse de déplacement du stylo, la pression exercée), l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier (vitesse de frappe).

I.4.3 La biométrie basée sur l'étude des traces biologiques

Elle est basée sur l'analyse des caractéristiques biologiques d'une personne tel que l'ADN, le sang, la salive, l'odeur, l'urine, …etc.

I.5 Les Techniques de la biométrie [4]

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, et qui exploitent diverses informations biométriques à savoir : l'empreinte digitale, le visage, la main, l'iris, la voix, la signature …

Nous donnons ici un aperçu des techniques biométriques les plus utilisé.

I.5.1 L'iris

La reconnaissance de l'iris est une technologie récente. L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d'un même individu sont différents. L'iris n'est pas modifiable par intervention chirurgicale, ajouté à cela qu'on peut distinguer jusqu'à 244 points de comparaison dans un iris, ce qui fait de cette technologie l'une des technologies les plus fiables qu'il soit avec un taux d'erreur proche de 0 %.

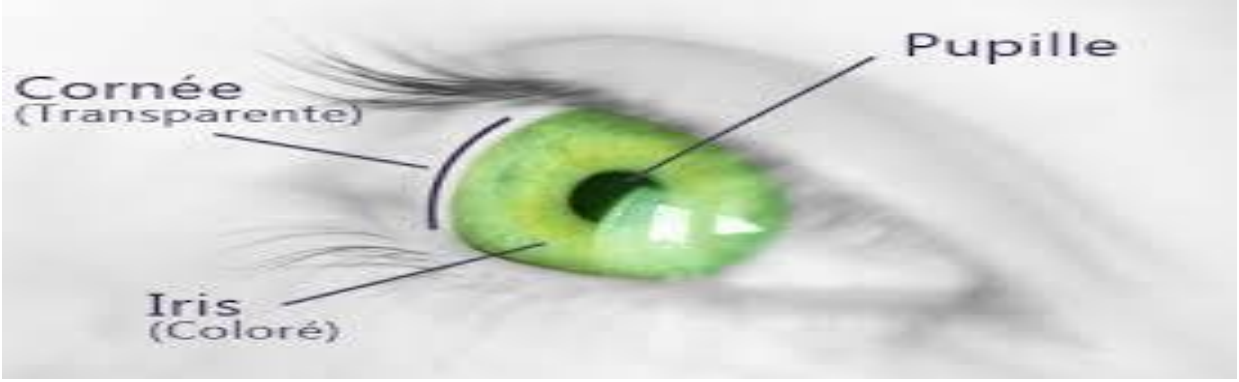


Figure I.1 : Détail d'une iris

Ces systèmes fonctionnent tout en capturant une image de l'iris avec un appareil à l'aide d'une lumière infrarouge, et en extrant les caractéristiques de l'iris qui sont comparés à un ou plusieurs gabarits.

Figure I.2 : Capteur d'images de l'iris

I.5.2 La géométrie de la main

Ce type de mesure biométrique est l'un des plus répandus et simples d'usage, elle consiste à déterminer les caractéristiques de la main d'un individu : sa forme, sa longueur, sa largeur, sa courbure des doigts, etc.

L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à positionner ses doigts, une photo de la face de la main est ensuite prise par un appareil photo numérique. Une photo de profile peut aussi être prise pour obtenir de l'information sur l'épaisseur de la main.

La géométrie de la main a un faible pouvoir, ce qui la rend inadaptée pour des applications d'identification. Elle offre un taux d'erreur relativement haut et elle n'est pas utilisable avec des personnes jeunes ou âgées.

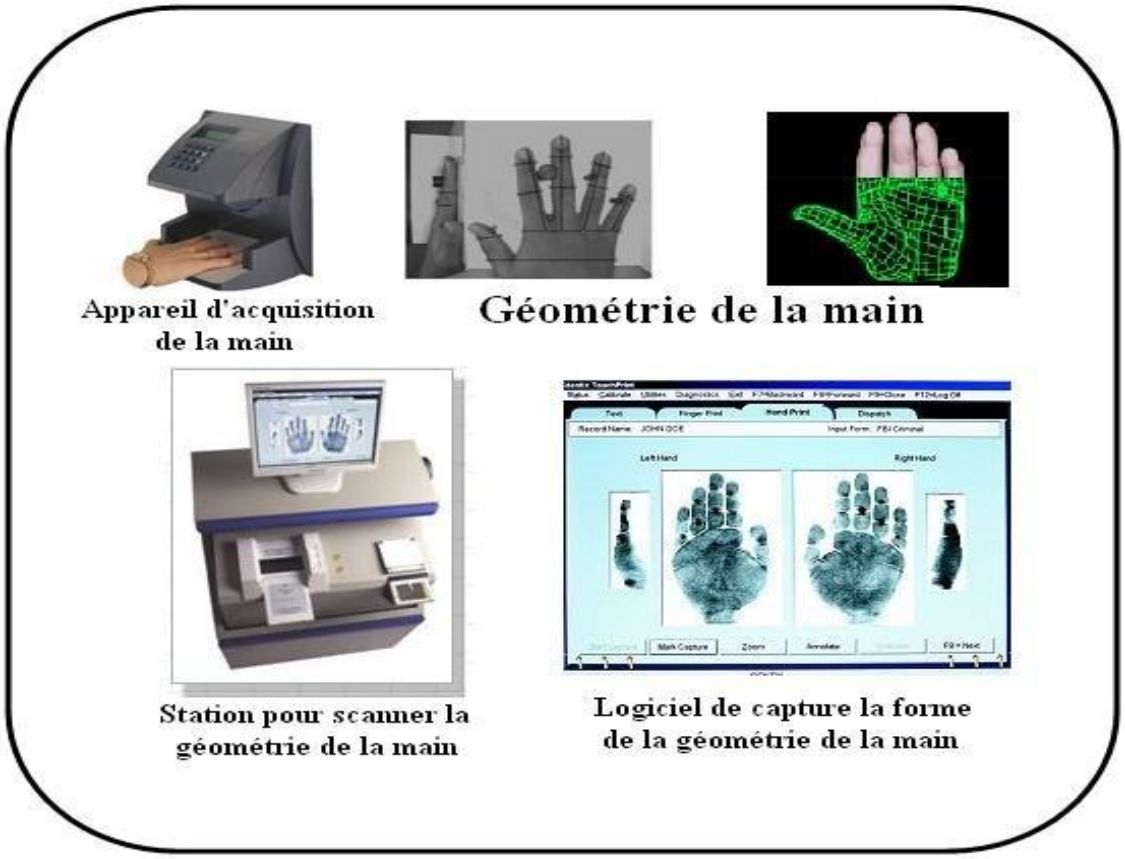


Figure I.3: Différents appareils de captures de la géométrie de la main.

I.5.3 La voix

La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mot de passe “pass-phrase”. Un téléphone ou un microphone peut être utilisé comme dispositif d’acquisition, ce qui rend cette technologie relativement économique et facilement réalisable, cependant elle peut être perturbée par des facteurs extérieurs comme le bruit de fond.

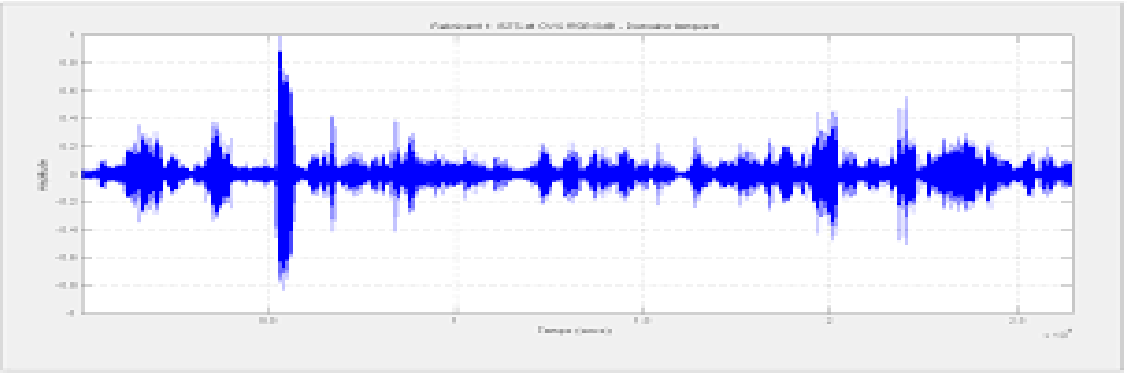


Figure I.4 : Spectre d’un signal voix.

I.5.4 La signature

La vérification par signature est une méthode automatique de mesure des signatures des personnes. Cette technologie examine un ensemble de dynamiques comme la vitesse, la direction, et la pression de l'écriture, le temps pendant lequel le stylo est en contact avec le papier, le temps pris pour faire la signature et les positions où le stylo est relevé et abaissé sur le papier.

Figure I.5 : Tablette Graphique

I.5.5 Acide Désoxyribose Nucléique (ADN) :

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'Acide Désoxyribonucléique (ADN), constituant essentiel des chromosomes du noyau cellulaire.

Selon les techniques d'analyse de l'ADN, l'identification est plus ou moins performante et/ou intrusive. L'identification d'un individu par analyse de son ADN s'avère complexe, coûteuse et lente à réaliser compte tenu des nombreuses manipulations biologiques (amplification + électrophorèse). Ceci explique qu'il n'existe toujours pas de solution technologique au grand-public qui permette de réaliser automatiquement cette analyse, d'autant plus qu'elle nécessite un prélèvement d'échantillon (sang, salive, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive.

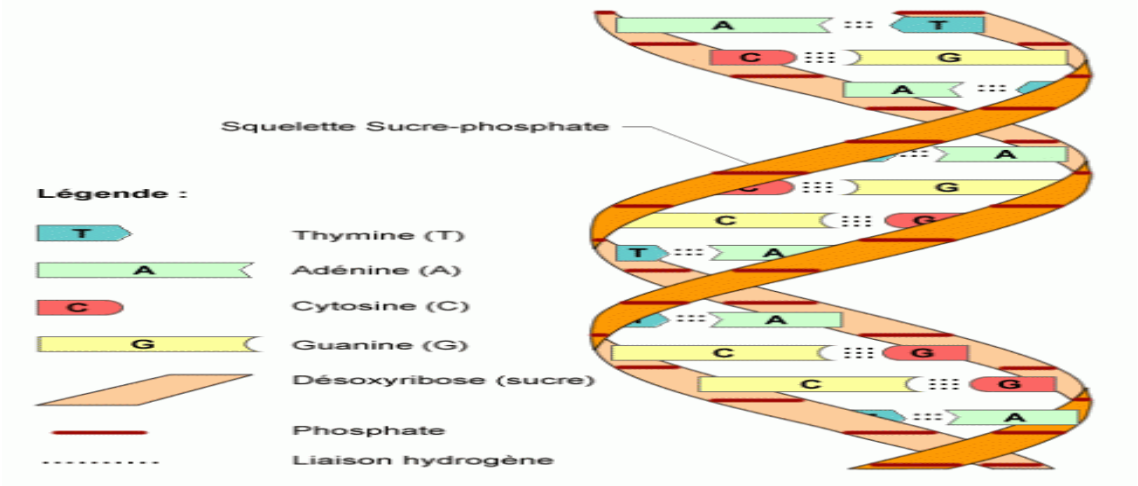


Figure I.6 : Structure de la molécule d'ADN

I.5.6 Empreinte digitale

I.5.6.1 Définition

La reconnaissance d'empreinte digitale est la technique biométrique la plus utilisée. Elle est utilisée depuis un siècle pour l'identification criminelle. Elle correspond à l'essentiel du marché actuel et son utilisation sera sans doute amenée à se développer. Elle possède un taux de fiabilité suffisant pour permettre d'identifier les individus dans de grandes bases de données. Utilisée depuis longtemps dans le contexte judiciaire, elle n'est pas toujours très bien acceptée par les utilisateurs à cause de l'association qui est

souvent faites avec la criminologie. Néanmoins, elle présente un bon compromis entre les contraintes d'utilisation et la fiabilité recherchée.

Les empreintes digitales sont uniques à chaque individu, en effet on estime à 1/64 milliard la probabilité pour que deux individus aient les mêmes empreintes digitales.

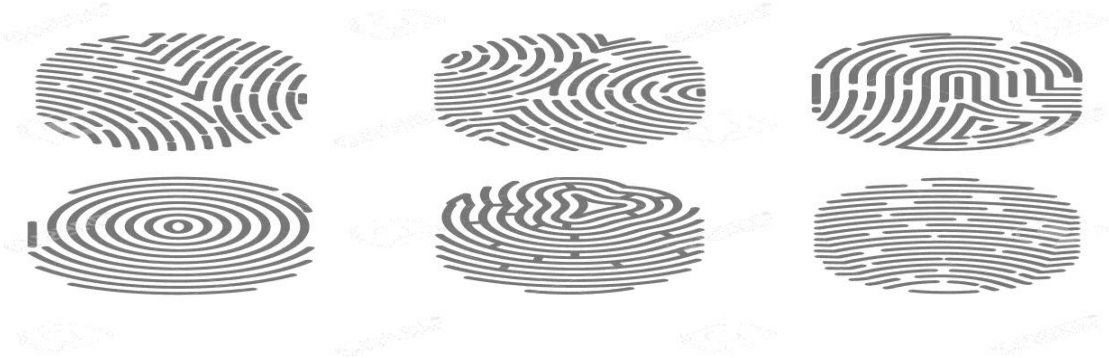


Figure I.7 : images des différentes classes d'empreintes digitales

I.5.6.2 Principe de fonctionnement

L'authentification par les empreintes digitales repose sur la concordance entre le fichier d'enregistrement, ou « signature », obtenu lors de l'enrôlement et le fichier obtenu lors de l'authentification. Ces deux fonctions se décomposent chacune en plusieurs étapes :

Fonction l : Enregistrement(enrôlement) :

- Capture de l'image de l'empreinte. Les données d'un doigt sont en principe suffisantes à l'enrôlement, mais la plupart des systèmes enregistrent au moins deux doigts (un par main par exemple) pour parer l'indisponibilité résultant de petites blessures.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Enregistrement sur un support, (carte à puce, disque dur...).

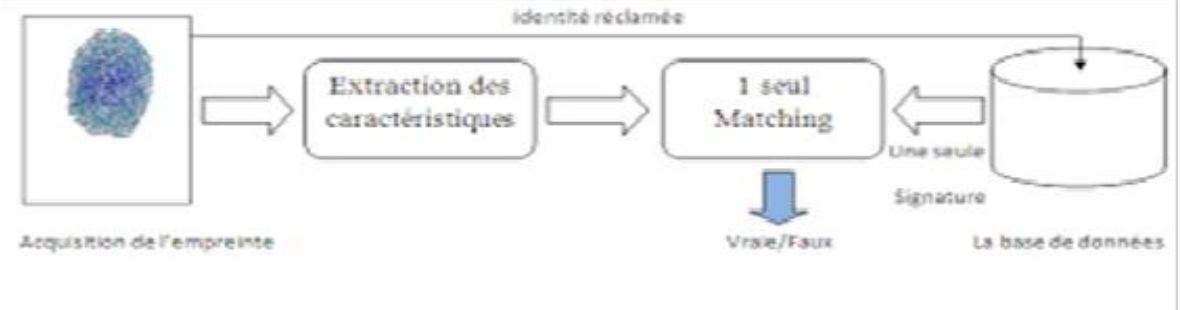


Figure I.8 : phase d'enregistrement d'une empreinte digitale.

Fonction 2 : Authentification :

- Capture de l'image de l'empreinte.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Comparaison entre l'échantillon et le gabarit « signature ».
- Prise de décision.

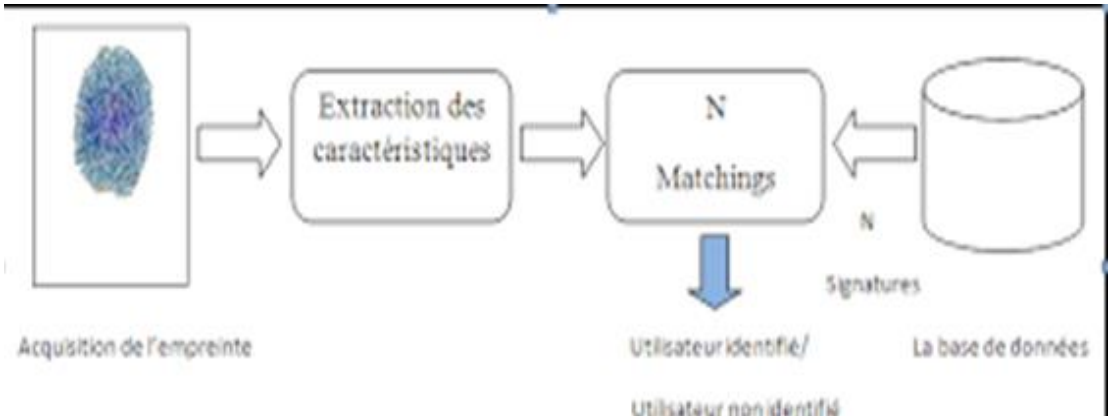


Figure I.9 : phase d'authentification d'une empreinte digitale.

- **Etapes de traitement :**

Lorsque la capture de l'image est réalisée, elle doit être convertie dans un format approprié. L'extraction des minuties est réalisée grâce à différents algorithmes. Il s'agit ensuite par une technique mathématique (segmentation) d'éliminer les informations non utiles au système : niveau de bruit trop élevé (image sale, doigt mal placé). L'image est numérisée afin de localiser précisément les terminaisons et les bifurcations, les crêtes sont affinées de 5 à 8 pixels à 1 pixel (à voir plus en détail dans le chapitre qui suit).

I.6 Etat du marché de la biométrie [5]

Un rapport sur le marché de la biométrie est édité par IBG (International Biometric Group). Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur.

La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investissements dans les entreprises biométriques, ou les développeurs de solutions biométriques. Le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes

d'information (ordinateur/réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.

On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physiques et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens).

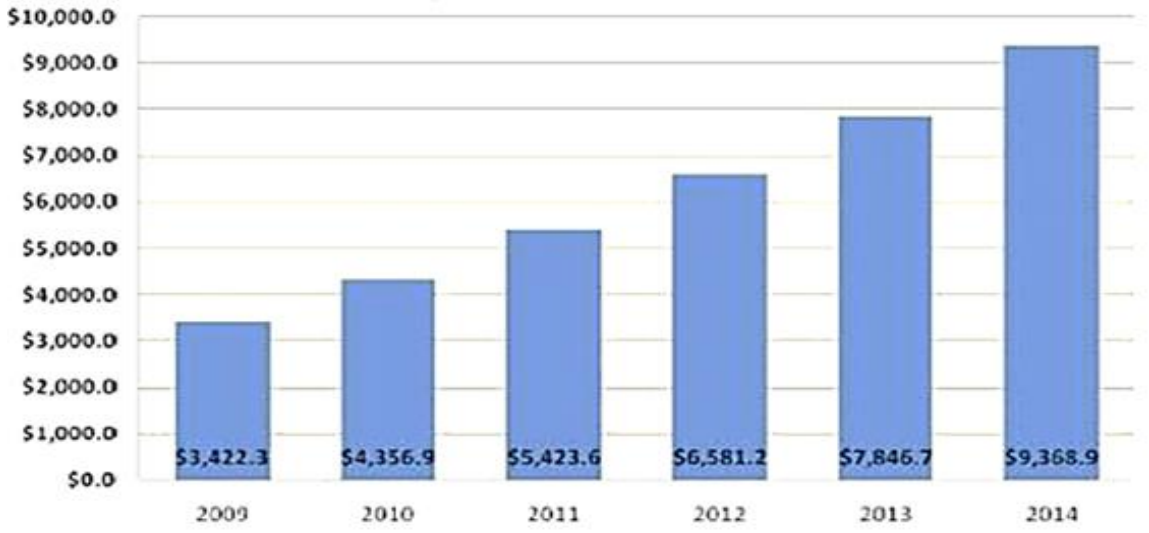


Figure I.10: Evolution du marché international de la biométrie.

I.7 Les parts de marché par technologies [6]

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50% du chiffre d'affaires total, dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de sources de revenus après les empreintes digitales.

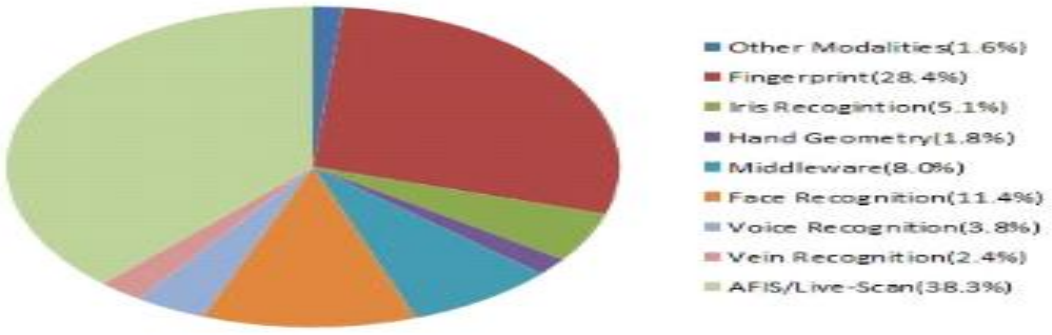


Figure I.11 : Parts de marché des différentes méthodes biométriques.

I.8 Conclusion

À travers ce chapitre nous avons pu développer le vaste sujet sur la généralité en rapport avec la biométrie et leurs domaines d'application, un survol sur les catégories biométriques ainsi que les technologies des systèmes biométriques.

La reconnaissance d'empreinte digitale est l'une des biométries les plus utilisées. C'est cette technique que nous avons préconisé pour notre contrôleur d'accès. Elle fera l'objet du chapitre suivant.

Chapitre II

L'empreinte digitale

II.1 Introduction

La Reconnaissance des empreintes digitales est une branche de la biométrie la plus rependue, aussi bien dans le domaine de la sécurité publique (contrôle, enquête), que privée (accès à un domicile, protection de biens…).

Les systèmes de reconnaissances des empreintes digitales sont utilisés dans plusieurs applications par exemples : sécuriser l'accès à un ordinateur, et dans le domaine de la criminologie, les services de la police scientifique utilisent l'empreinte digitale comme moyen d'identification d'une personne depuis plus de 100 ans.

Le principe de la reconnaissance des empreintes digitales consiste à comparer 2 empreintes fournies au système à une ou plusieurs autres empreintes aussi appelé « Template » ou signatures, le système biométrique renvoie un résultat positif au cas où l'empreinte fournie à l'entrée correspond à l'un des Template, et un résultat négatif dans le cas contraire.

II.2 Historique [7]

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de l'époque des pyramides il y a plus de 4000 ans. Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient sûrement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable. C'est en 1856 que l'anglais William Hershel, après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, commença à comprendre que les empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (Unicité, Les empreintes furent adoptées officiellement en Angleterre dans le système judiciaire.

Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires. De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable.

II.3 Représentation des empreintes digitales [8]

Le problème de la représentation constitue l'essence dans la création des systèmes de reconnaissance automatique des empreintes digitales et a des implications énormes sur le design du reste du système. Une bonne représentation d'une empreinte digitale doit être saillante et pertinente. Saillante signifie que cette représentation contient des informations distinctives sur l'empreinte digitale tandis que pertinente signifie qu'elle

peut être facilement extraite, stockée d'une façon compacte et utile pour la comparaison plus tard. La caractéristique structurelle la plus évidente dans les empreintes digitales est la forme des crêtes et vallées ; dans une image d'empreinte digitale, les lignes de crêtes sont sombres alors que les lignes de vallées sont claires (voir Figure).

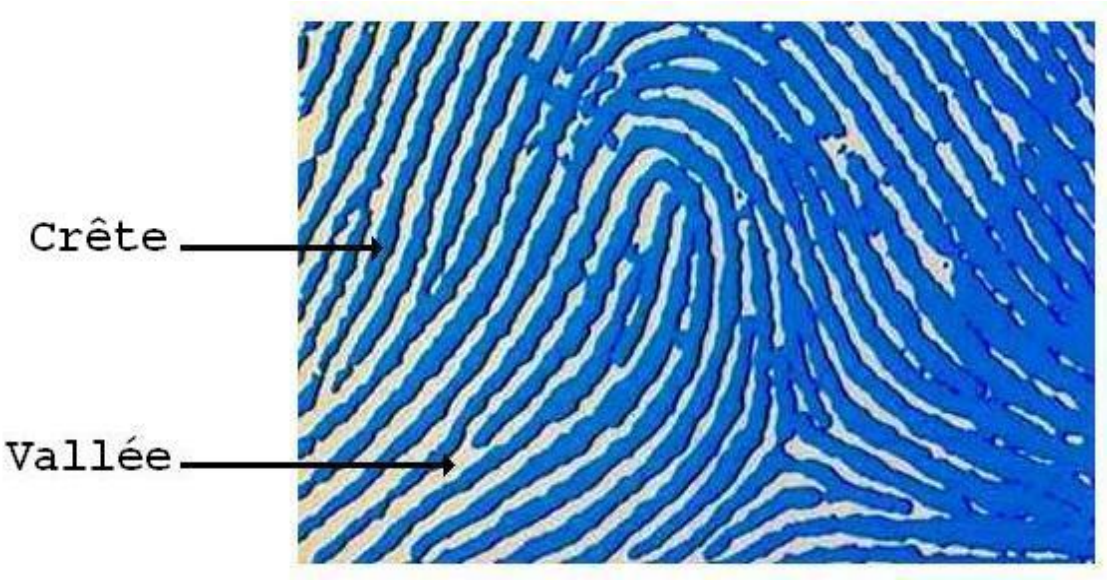


Figure II.1 : Les Vallée et crêtes d'une empreinte digitale.

II.3.1 Les points caractéristiques de l'empreinte digitale

Les pointes caractéristiques ou les crêtes sont utilisées pour différencier deux empreintes digitales et aussi faires une classification selon les points singuliers globaux et les points singuliers locaux.

II.3.1.1 Les points singuliers globaux

On distingue les points caractéristiques globaux par le Core et le Delta.

•**Le Core** : centre ou le noyau contient les courbures maximales des lignes de l'empreinte.

•**Le Delta** : le lieu de divergence des lignes les plus internes.

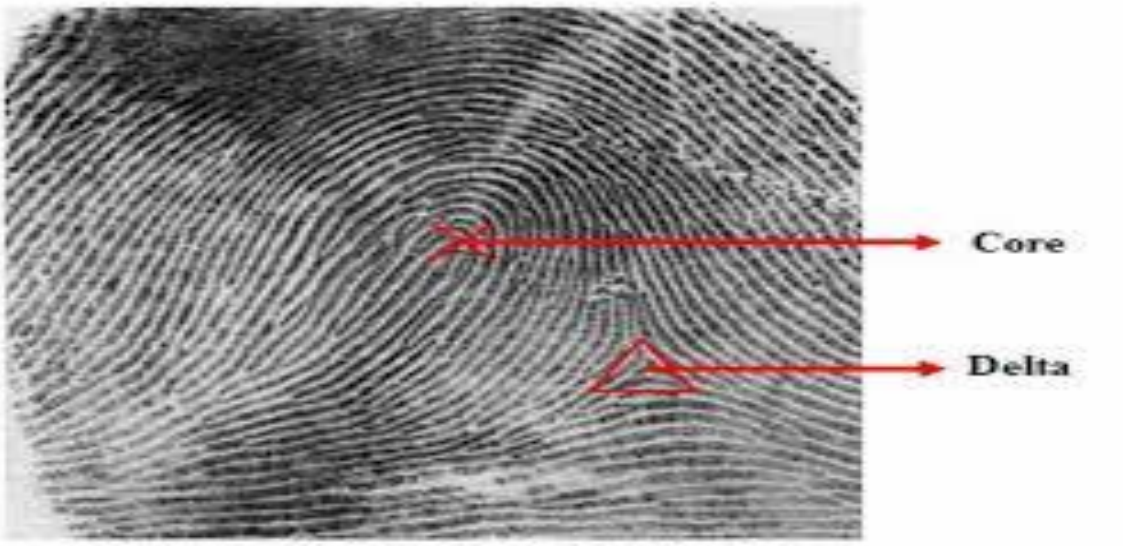


Figure II.2 : les points singuliers globaux d'une empreinte digitale

II.3.1.2 Les points singuliers locaux (minutiers)

•**Les coupures** : terminaison à droite ou à gauche, minuties situées en fin de stries.

•**Les divisions** : Bifurcation à droite ou à gauche, intersection de deux stries.

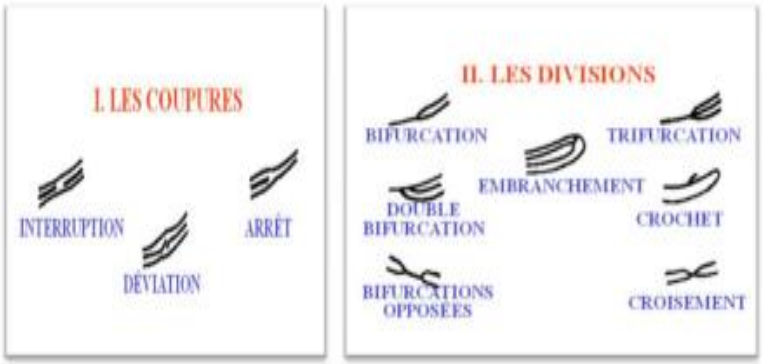


Figure II.3 : Les coupures et les divisions.

•**Les anneaux** : Lac, assimilée à deux bifurcations.

•**Les ilots** : assimilés à deux terminaisons.

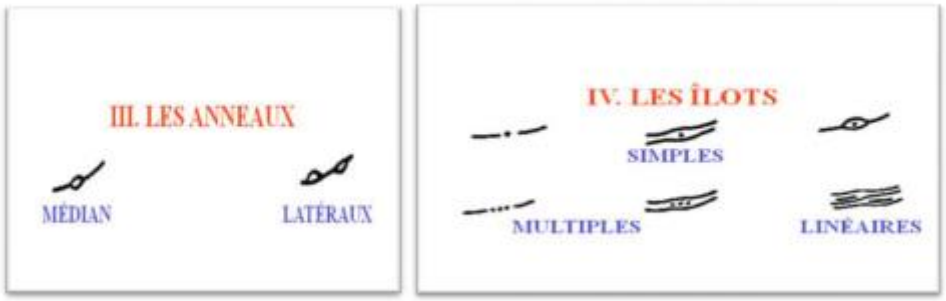


Figure II.4: Les anneaux et les ilots.

II.4 Structure d'un système complet de reconnaissance d'empreintes [9]

II.4.1 Principe général

Un système automatique complet de reconnaissance d'empreintes digitales est une chaîne de processus qui, à partir du doigt d'un utilisateur en entrée, renvoie un résultat en sortie, permettant ainsi à l'utilisateur d'accéder ou non à des éléments nécessitant une protection. La réalisation d'un tel système a fait l'objet de très nombreuses recherches et des méthodes très différentes de traitement ont été proposées. Cependant ces systèmes répondent toujours à la même structure.

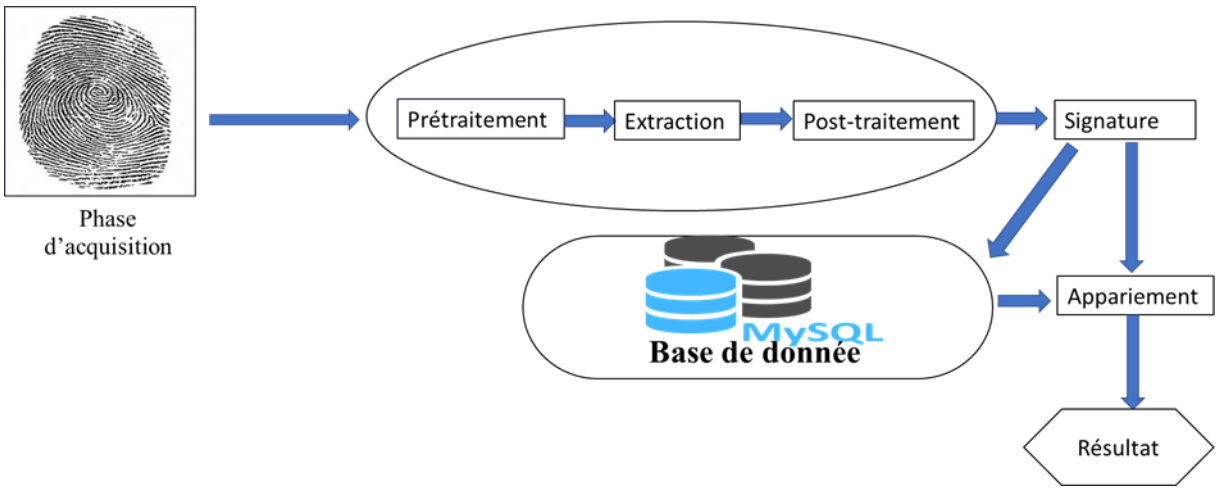


Figure II.5 : Architecture générale d'un système complet de reconnaissance d'empreintes.

La première phase permet d'obtenir une image de l'empreinte de l'utilisateur (acquisition), laquelle va subir un prétraitement pour extraire l'information utile de l'image (signature) suivi éventuellement d'un traitement supplémentaire permettant d'éliminer de possibles fausses informations qui se seraient glissées entre temps dans la chaîne de traitement.

Ensuite si l'utilisation du système consiste juste à créer une base de données (stockage) la signature est éventuellement compressée puis stockée dans la base de données au moyen d'une technique d'archivage (classification).

Pour un système d'identification, l'ensemble des empreintes présentes dans la base de données pouvant correspondre à celle de l'utilisateur (modèle identique) sont désarchivées et comparées (appariement) une à une avec celle de l'utilisateur, si une éventuelle correspondance est trouvée, des informations personnelles concernant l'utilisateur sont renvoyées par le système. Dans le cas d'un système de vérification, il n'y a qu'une seule comparaison et un résultat binaire est renvoyé, permettant l'acceptation ou le rejet de l'utilisateur.

II.4.1.1 L'acquisition de l'empreinte

L'acquisition d'empreinte consiste à capturer les images numériques d'empreintes et extraire les lignes tracées par les crêtes (en contact avec le capteur) et les vallées. La qualité d'image de l'empreinte digitale peut varier selon que la peau du doigt est sale, trop humide ou trop sèche, huileuse ou affligée d'une coupure. La pression que l'on exerce sur le lecteur optique de l'appareil est aussi déterminante quant aux détails qui sont recueillis. Un bon système biométrique tiendra compte de ces facteurs. Le point commun à toutes les technologies utilisées pour la prise d'image d'une empreinte, est que l'image est constituée à partir des points de contact du doigt sur le capteur. Les techniques d'acquisition sont diverses on citera :

II.4.1.1.1 Les capteurs optiques d'empreinte

La méthode optique est une des méthodes les plus communes. Un appareil-photo CCD (Dispositif Charge Couplé) est utilisé au cœur du capteur optique. Un appareil-photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photo sites. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED qui illumine les creux et les bosses du doigt. Le prix constitue l'avantage principal des systèmes optiques ; leur inconvénient est qu'ils sont faciles à détourner. L'autre problème est celui des empreintes latentes : l'empreinte digitale du doigt précédente, qui a été placé sur le capteur, peut rester

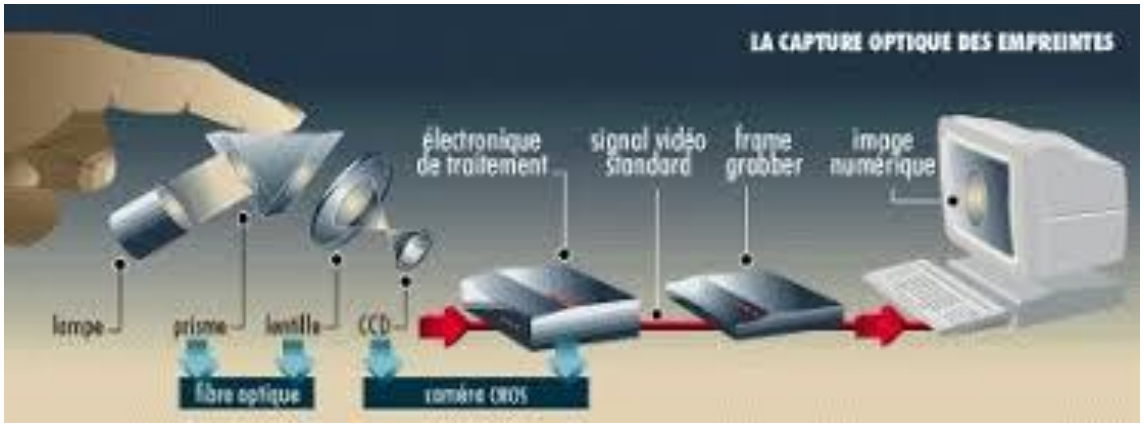


Figure II.6 : capteur optique.

II.4.1.1.2 Capteurs capacitifs

La méthode capacitive est l'une des méthodes les plus populaires. Comme les autres capteurs, le capteur capacitif reproduit l'image des creux et des bosses qui composent une empreinte digitale. Le capteur capacitif emploie des condensateurs de courant électrique pour mesurer l'empreinte, il se compose d'une rangée de cellules minuscules. Chaque cellule inclut deux plaques conductrices recouvertes par un revêtement protecteur. L'avantage principal de ces capteurs est qu'ils demandent une réelle empreinte digitale. Mais ils rencontrent des difficultés avec les doigts secs et humides.

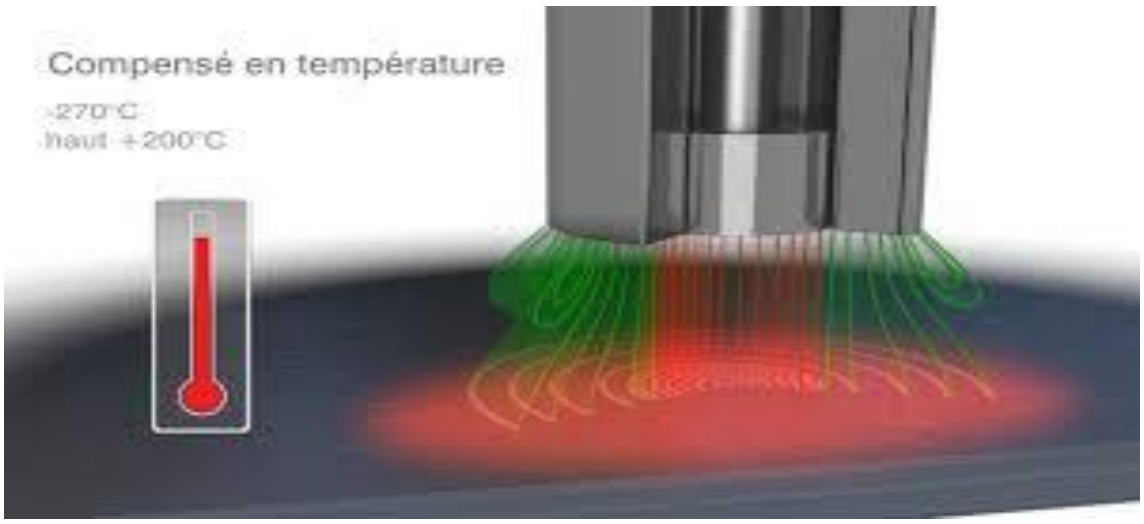


Figure II.7 : Capteur capacitifs

II.4.1.1.3 Capteurs de champ-électrique

Ce capteur fonctionne avec un champ-électrique et le mesure au-delà de la couche extérieure de la peau où l'empreinte digitale commence. Cette technologie peut être utilisée dans des conditions extrêmes, c'est-à-dire même si le doigt est sale ou sec. La technologie de champ-électrique crée un champ entre le doigt et le semi-conducteur adjacent qui imite la forme des creux et des bosses de la couche épidermique du doigt. Un amplificateur de sousPixel est utilisé pour mesurer les signaux. Les capteurs fonctionnent ensemble afin de rendre une image plus claire correspondant exactement au modèle de l'empreinte digitale.

On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. L'inconvénient est la basse résolution d'images et une trop petite zone d'image, ce qui a pour conséquence de générer un haut taux d'erreur.

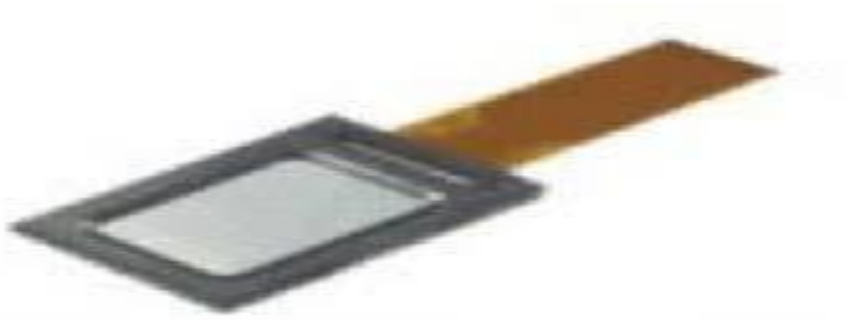


Figure II.8 : Capteur de champ électrique.

II.4.1.2 Le prétraitement de l'image

Les algorithmes de reconnaissance des empreintes digitales sont sensibles à la qualité des images d'empreintes digitales obtenues lors de l'acquisition. La qualité de ces images dépend de plusieurs facteurs comme, les substances parasites présentes sur le doigt (encre, graisse, saletés…). La personne (cicatrices, métiers manuels, âge…). L'environnement où se produit l'acquisition (température de l'air, degré d'humidité…) et les caractéristiques spécifiques du moyen d'acquisition utilisé, la profondeur de rides/vallée, etc. Alors l'étape de prétraitement est nécessaire avant d'effectuer les étapes suivantes. Typiquement le prétraitement peut se composer de lissage, de segmentation et de filtrage du domaine spatiale/ fréquence.

II.4.1.3 L'extraction de la signature

La plupart des systèmes de reconnaissance des empreintes digitales emploient des minuties comme caractéristiques des empreintes digitales. Un extracteur de minuties cherche des terminaisons de stries et des bifurcations dans les empreintes. Si les stries

sont bien déterminées, alors l'extraction de minuties est une tâche relativement simple. Cependant, dans la pratique, il n'est pas toujours possible d'obtenir une carte parfaite de stries. Donc la performance des algorithmes d'extraction de minuties dépend fortement de la qualité des images des empreintes digitales d'entrées.

II.4.1.4 Le stockage et la phase d'appariement

Pour les systèmes disposant de grosses bases de données, l'identification peut poser un problème en temps de calcul si la signature d'entrée doit être comparée avec les signatures présentes dans la base donnée. C'est pourquoi, un processus de classification et de déclassification est nécessaire pour limiter les temps de recherche.

Lorsqu'une image est stockée, un groupe spécifique lui est attribué en fonction de ses caractéristiques. Lors de l'identification, on désarchive l'ensemble des signatures de la base correspondant au groupe de l'empreinte nécessitant l'identification. Puis chacune des images désarchivées est comparée avec celle de l'utilisateur. Ceci permet de réduire sensiblement le temps de recherche en limitant le nombre d'images à comparer.

Parmi les différentes techniques existantes on distingue principalement : l'extraction des singularités de l'image (la position des centres et delta permet de déterminer la classe de l'empreinte). La phase d'appariement est l'étape critique du système, elle reçoit en entrée deux signatures issues de deux acquisitions différentes d'empreinte et renvoie en sortie un résultat binaire indiquant si oui ou non les deux signatures proviennent de la même empreinte.

II.5 Conclusion

Dans ce chapitre nous avons vu les caractéristiques des empreintes digitales ainsi que la description de la structure globale d'un système de reconnaissance d'empreintes ont également été décrits ; il s'agit à l'heure actuelle de la technique biométrique la plus aboutie.

Notre système de reconnaissance d'empreintes digital doit s'intégrer facilement dans une Smart home à travers le protocole de communication I2C. Dans le prochain chapitre, nous allons mettre l'accent sur la smart homes, ses différents protocoles ainsi que les systèmes embarqués sur lesquels ils reposent.

Chapitre III

L'Etat de l'art sur les systèmes embarqués et la Smart Home

III.1 Introduction

De nos jours, la maison intelligente est devenue un paradigme assurant une vie d'extrême confort et de modernisme. Ainsi avec le développement que l'électronique et la nanotechnologie ont connu, tout est devenu miniature et accessible. De plus, grâce à l'informatique et la programmation, les systèmes embarqués ont pris de l'ampleur et se sont attaqués à tous les domaines notamment la Smart house.

III.2 Définition de système embarqué [10]

Un système embarqué est un système électronique ayant une architecture d'ordinateur autonome ne possédant pas des entrées/sorties standards comme un clavier ou un écran d'ordinateur. Il est piloté par un logiciel, qui est complètement intégré au système qu'il contrôle.

III.3 Caractéristiques [11]

Chaque système embarqué a des caractéristiques spécifiques parmi eux on cite quelques-unes :

- ✓ Dédié à une application spécifique
- ✓ Coût réduit, maximisation rapport performance/prix
- ✓ Volume restreint (compact, pas modulaire)
- ✓ Capacité mémoire adaptée
- ✓ Capacité de calcul appropriée à l'application
- ✓ Exécution temps réel (souvent)
- ✓ Fiabilité et sécurité de fonctionnement
- ✓ Consommation d'énergie maitrisée

III.4 Applications de systèmes embarqués [12]

Les systèmes embarqués sont introduits dans divers domaines, à savoir :

- **Le domaine grand public :**
  Smart phone, console de jeux, appareil photos, lecteur audio
- **Les moyens de transport :**
  Ordinateur de bord, GPS, système de navigation, automobiles, avions, trains, bateau
- **Les équipements médicaux :**
  Imagerie (rayon X, ultra-sons, IRM) endoscopie, caméra, monitoring, perfusion, lasers, chirurgie, stimulateur cardiaque

- **Les équipements de télécommunication :**
  Station mobile, routeur, gateway, satellite
- **Les équipements industriels :**
  Productions automatisées, systèmes de commande d'énergie, équipements de stockage
- **Les équipements de bureautiques :**
  Répondeurs, copieurs, imprimante.
- **Les équipements de bâtiment :**
  Ascenseurs, système de surveillance, contrôle d'accès, systèmes d'éclairage, smart home…

III.4.1.1 Définition smart home [13]

Smart Home (La maison intelligente) ou Domotique est l'évolution logique d'une maison possédant de nombreuses connectivités. On dirait qu'il s'agit d'un concept performant mettant en action l'ensemble des techniques et technologies électroniques, informatiques permettant d'automatiser et d'optimiser les tâches au sein d'une maison sans aucune intervention humaine, utilisées dans les bâtiments, pour centraliser le contrôle des différents systèmes et sous-systèmes de la maison (chauffage, porte de garage, portail d'entrée, prises électriques, etc.).

La Smart Home vise à apporter des solutions techniques pour répondre aux besoins de confort (gestion d'énergie, optimisation de l'éclairage et du chauffage), de sécurité (alarme) et de communication (commandes à distance, signaux visuels ou sonores, etc.) que l'on peut retrouver dans les maisons, les hôtels, les lieux publics, etc…

Figure III.1 : La Smart Home

III.4.1.2 Différents domaines d'application de la domotique [14]

On peut dire que la domotique trouve sa place dans quatre domaines principaux en particulier :

III.4.1.2.1 Le confort

Grace à la domotique, on peut gérer les équipements d'une maison (l'éclairage, gestion du chauffage, gestion des volets roulants) avec une simple commande et sans déplacement, Par exemple, vous n'avez plus à aller ouvrir le portail, Il suffit d'appuyer sur un bouton de commande et votre portail s'ouvre et se referme automatiquement. Grâce à une application sur votre Smartphone.

Figure III.2 : domaine de confort de la domotique

III.4.1.2.2 La sécurité

Afin de protéger et sécuriser une maison, il est possible de simuler une présence. Du coup il est difficile de discerner si la maison est occupée ou non, ce qui permet de dissuader les cambrioleurs.

Par ailleurs, les systèmes d'alarmes connectées peuvent vous alerter en cas d'intrusion dans votre domicile. La présence de caméra de surveillance connectée à votre Smartphone vous permet en outre de visualiser en permanence ce qui se passe chez vous. Ce qui peut aussi dissuader les personnes qui ont de mauvaises intentions.

Figure III.3 : domaine de sécurité de la domotique.

III.4.1.2.3 Economie d'énergie

En gérant les volets selon la saison, ainsi que le chauffage, le système domotique vous permet d'économiser de l'énergie, et donc de l'argent, même si au départ on ne recherchait que le confort. La consommation d'énergie peut être suivie très finement, qu'il s'agisse de votre consommation d'électricité, d'eau, ou même de gaz. Le simple fait d'activer l'alarme en partant va passer le chauffage en mode éco, et éteindre toutes les lampes et les appareils restés en veille, réduisant ainsi votre consommation d'énergie en votre absence. Et ceci sans aucune action de votre part.

Figure III.4 : Domaine d'économie d'énergie de la domotique

III.4.1.2.4 La Communication

Un système domotique permet la communication non seulement à l'intérieur de la maison, mais aussi à l'extérieur.

La technologie Internet interviendra de plus en plus pour la commande à distance par certains utilisateurs. Vous ne devez même pas être à la maison pour commander vos appareils. Un simple coup de fil ou un sms vous permettra par exemple de régler le chauffage à distance, d'activer une simulation de présence ou de lancer le lave-vaisselle ou le lave-linge.

Figure III.5 :HomeChat

III.4.1.3 Avantages et Inconvénients de la smart home [15]

III.4.1.3.1 Avantages

Parmi les principaux avantages de la smart home on trouve :

- L'amélioration du quotidien au sein de la maison, du point de vue du confort, de la sécurité et de la gestion de l'énergie.
- Simplifie la vie et optimise votre confort en adaptant votre maison à différents scénarios de la vie quotidienne.
- Il vous permet notamment d'éteindre tous vos appareils électriques et de mettre l'alarme quand vous quittez votre domicile, de régler des ambiances lumineuses (ambiance lecture, ambiance relaxation avec lumières tamisées), de vous réveiller dans un habitat chauffé où le café est déjà prêt, d'enclencher automatiquement l'arrosage ou l'ouverture des volets chaque matin.
- La domotique permet aussi de réaliser des économies d'énergie grâce à la gestion automatique du chauffage, de la climatisation et de l'éclairage et à la programmation des appareils électroménagers en heures creuses.
- Elle a pour avantage d'améliorer la sécurité grâce à des alarmes, des systèmes d'ouverture automatique de la porte (reconnaissance vocale, carte magnétique…)
- En cas de tentative d'intrusion dans la maison, un appel téléphonique automatique peut contacter le propriétaire ou une entreprise de sécurité.
- Enfin, ces différentes technologies constituent une aide précieuse pour les personnes dépendantes et handicapées.

III.4.1.3.2 Inconvénients

- Prix d'achats, et d'installations.
- Le verrouillage qu'offrent certaines marques dans leurs produits ne permettant pas d'avoir un logiciel ouvert.

III.5 Les protocoles de communication de la Smart home

Un protocole de communication d'une maison intelligente est un moyen défini pour les équipements de communiquer. Les appareils qui parlent la même langue peuvent se parler et être contrôlés via une seule application. Les appareils qui utilisent différents protocoles sont contrôlés via des applications séparées et ne peuvent pas communiquer. Pour cette raison, certaines entreprises ont utilisé des protocoles standard (tels que Z-Wave, Zigbee ou Wi-Fi) pour permettre aux appareils de fonctionner ensemble et d'être contrôlés via une seule application.

III.5.1 Différents protocoles de communications

III.5.1.1 Bluetooth [16]

Protocole sans fil à courte portée (environ 10 m) souvent utilisé sur les téléphones, les écouteurs et les haut-parleurs. Son système de sauts de fréquence adaptatif évite les interférences avec les réseaux existants, tels que le Wifi, et négocie une carte des canaux pour les périphériques Bluetooth.

Figure III.6: le logo de protocole Bluetooth

III.5.1.2 Wi-Fi [17]

Compte tenu de l'omniprésence du Wi-Fi dans l'environnement domotique au sein de réseaux locaux, la connectivité Wi-Fi s'impose souvent comme le choix évident pour beaucoup de développeurs. Elle offre plusieurs avantages comme la vaste infrastructure

existante, le transfert de données rapide et la possibilité de gérer de grandes quantités de données.

À l'heure actuelle, la 802.11n s'impose comme la norme Wi-Fi la plus utilisée dans le contexte privé et professionnel. Cette norme offre un débit élevé, de l'ordre de centaines de mégabits par seconde, idéale pour les transferts de fichiers, mais peut-être trop énergivore pour la plupart des applications IoT.

- Norme : basée sur 802.11n (actuellement la norme la plus utilisée pour un usage privé)
- Fréquences : bandes de 2,4 GHz et 5 GHz
- Portée : environ 50 m
- Vitesses de transmission : 600 Mbit/s maximum, mais les vitesses habituelles sont plus proches de 150 Mbit/s, en fonction de la fréquence de canal utilisée et du nombre d'antennes (la dernière norme 802.11-ac devrait permettre des vitesses pouvant atteindre 500 Mbit/s à 1 Gbit/s)

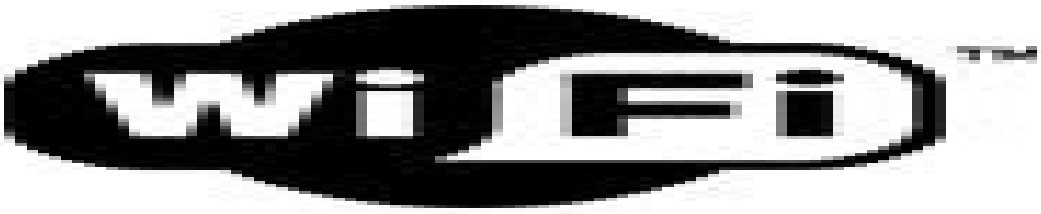


Figure III.7: le logo protocole Wifi.

III.5.1.3 KNX [18]

KNX est un protocole ouvert qui existe sur le marché depuis des décennies et qui est également l'un des protocoles les plus populaires pour l'automatisation des bâtiments. Il fonctionne sur plusieurs couches physiques, par exemple câblage à paires torsadées, réseau de lignes électriques, infrarouge, Ethernet et RF.

Avec une topologie décentralisée, le système ne fonctionne pas à partir d'une unité centrale, ce qui signifie que chaque unité reliée à l'écosystème KNX est intelligente en soi et ne dépend pas d'autres composants pour fonctionner. Un gros avantage : si une unité échoue, les autres peuvent toujours poursuivre leurs activités quotidiennes.

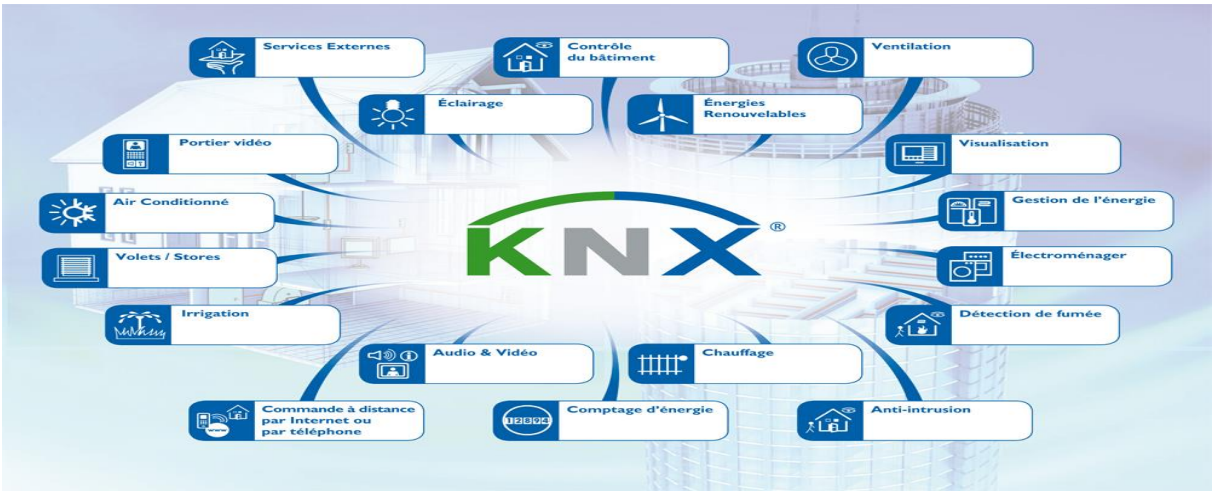


Figure III.8: le protocole KNX

III.5.1.4 Cpl (courant porteur en ligne) :[19]

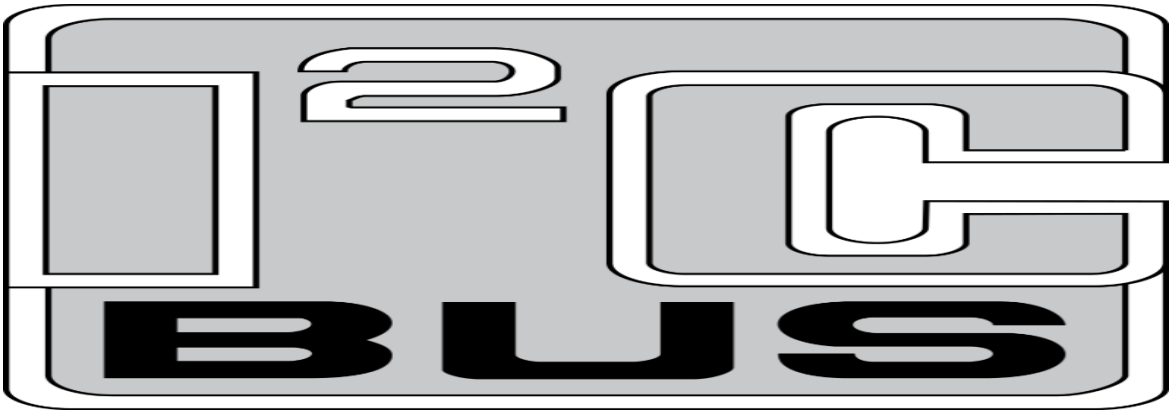
La technologie du courant porteur en ligne (CPL) permet le transfert et l'échange d'informations et de données en passant par le réseau électrique existant. L'installation est composée d'émetteurs et de récepteurs connectés au réseau électrique qui communiquent entre eux. Le principe de base du réseau CPL (Courant Porteur en Ligne) est d'utiliser les circuits de distribution électrique du bâtiment pour véhiculer des données et des commandes.

Figure III.9 : courant porteur en ligne.

III.5.1.5 I2C [20]

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

Dans le protocole du bus I2C le 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 équipement adressé est considéré comme un esclave.



FigureIII.10 : le logo de protocole I2C

III.5.1.5.1 Terminologie du bus I2C

- **Transmetteur :** Le circuit qui envoie la donnée sur le bus
- **Receveur** : Le circuit qui reçoit la donnée du bus
- **Maître** : Le circuit qui commence le transfert, génère l'horloge et terminele Transfert.

- **Esclave** : Le circuit adressé par le maître.

III.5.1.5.2 Caractéristiques générales

III.5.1.5.2.1 Caractéristiques physiques

- Deux fils SDA (Serial Data) et SCL (Serial Clock) véhiculent les informations entre les différents circuits.

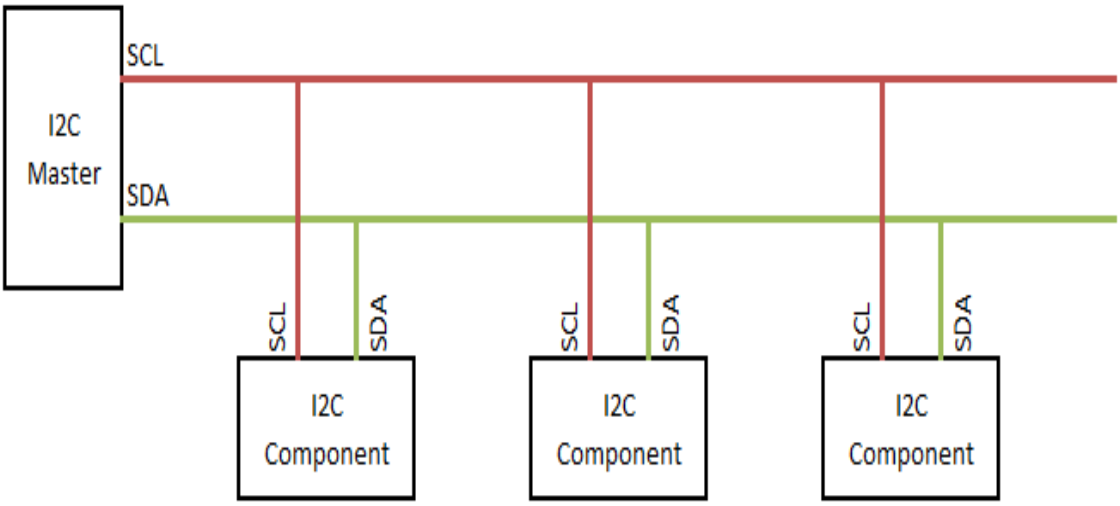


Figure III.11 : Caractéristique de I2C

SDA et SCL sont des lignes bidirectionnelles, connectées à plus VCC par l'intermédiaire de deux résistances de tirage. Quand le bus est libre, c'est à dire quand il n'ya pas de transfert de données les deux lignes sont à l'état haut 1.

III.5.1.5.2.2 Vitesse de transfert

Le transfert des données peut se faire jusqu'à une vitesse de 100 à 400 kbits /s.

III.5.1.5.2.3 Nombre maximal de circuits connectés

De part les contraintes d'adressage (7 bits ou 10 bits), le nombre maximal de circuits connectés sur le bus est en théorie entre 127 ou 1023. En pratique, le nombre dépend de la capacitance maximale du bus qui est de 400 pf.

III.5.1.5.3 Fonctionnement de protocole I2C

La communication sur le bus I²C ne peut se faire qu'entre 2 équipements à un moment donné.

Lorsqu'un équipement prend le contrôle du bus, il devient le maître de la communication. Il génère le signal d'horloge SCL et communique avec un esclave. Selon le sens de la communication, il sera l'émetteur ou le récepteur.

Lorsque aucun équipement n'émet sur le bus, les lignes SDA et SCL sont au niveau haut qui est leur état de repos.

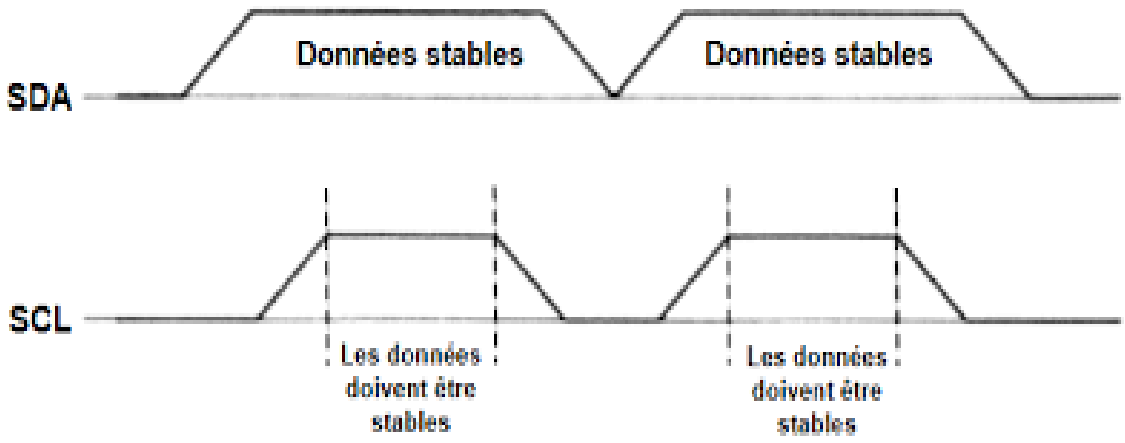


Figure III.12: le principe fondamental d'un transfert de données

Une donnée n'est considérée comme valide sur le bus que lorsque le signal SCL est à l'état haut. L'émetteur doit donc positionner la donnée à émettre lorsque SCL est à l'état bas et la maintenir tant que SCL est à l'état haut.

Comme la transmission s'effectue sous forme série, une information de début et de fin doit être prévue. L'information de début se nomme START et l'information de fin STOP.

III.6 Conclusion

Ce chapitre a été consacré à l'introduction des concepts des systèmes embarqués, et des Smart homes. Leurs caractéristiques ainsi que leurs différentes applications (industrielles, bâtiments...).

La smart home a débarqué récemment pour faciliter la vie quotidienne, mais cette technologie n'est pas à la portée de tout le monde à cause du prix. Toutefois, le développement des technologies embarquées et le cout de plus en plus réduits des microcontrôleurs peut aider à rendre les Smart home plus accessible au grand publique.

Notre projet s'inscrit dans ce cadre et permet d'utiliser un système embarqué à moindre cout pour réaliser un contrôleur d'accès à base de d'empreinte digitale intégrable dans une Smart home. Au cœur de ce système on trouve le microcontrôleur ESP32. Il est doté de plusieurs interfaces de communication dont le Wifi, le Bluetooth ainsi que le bus I2C. le chapitre suivant présente les étapes de conception de ce contrôleur d'accès.

Chapitre IV

Conception

IV.1 Introduction

L'objectif de notre travail est de réaliser un système de contrôle d'accès permettant l'ouverture automatique d'un accès à un domicile ou à une structure en utilisant l'empreinte digitale des personnes autorisées. Ce système communique avec une centrale de domotique et un serveur Web en utilisant le Wifi (pour l'accès au serveur Web) et le protocole I2C (pour communiquer avec une centrale de domotique).

IV.2 Schéma Synoptique global

La figure IV.1 donne le schéma synoptique global d'une centrale de domotique contenant plusieurs capteurs et actionneurs. Notre système sera considéré comme un actionneur de la centrale permettant d'ouvrir et de fermer automatiquement la porte du domicile.

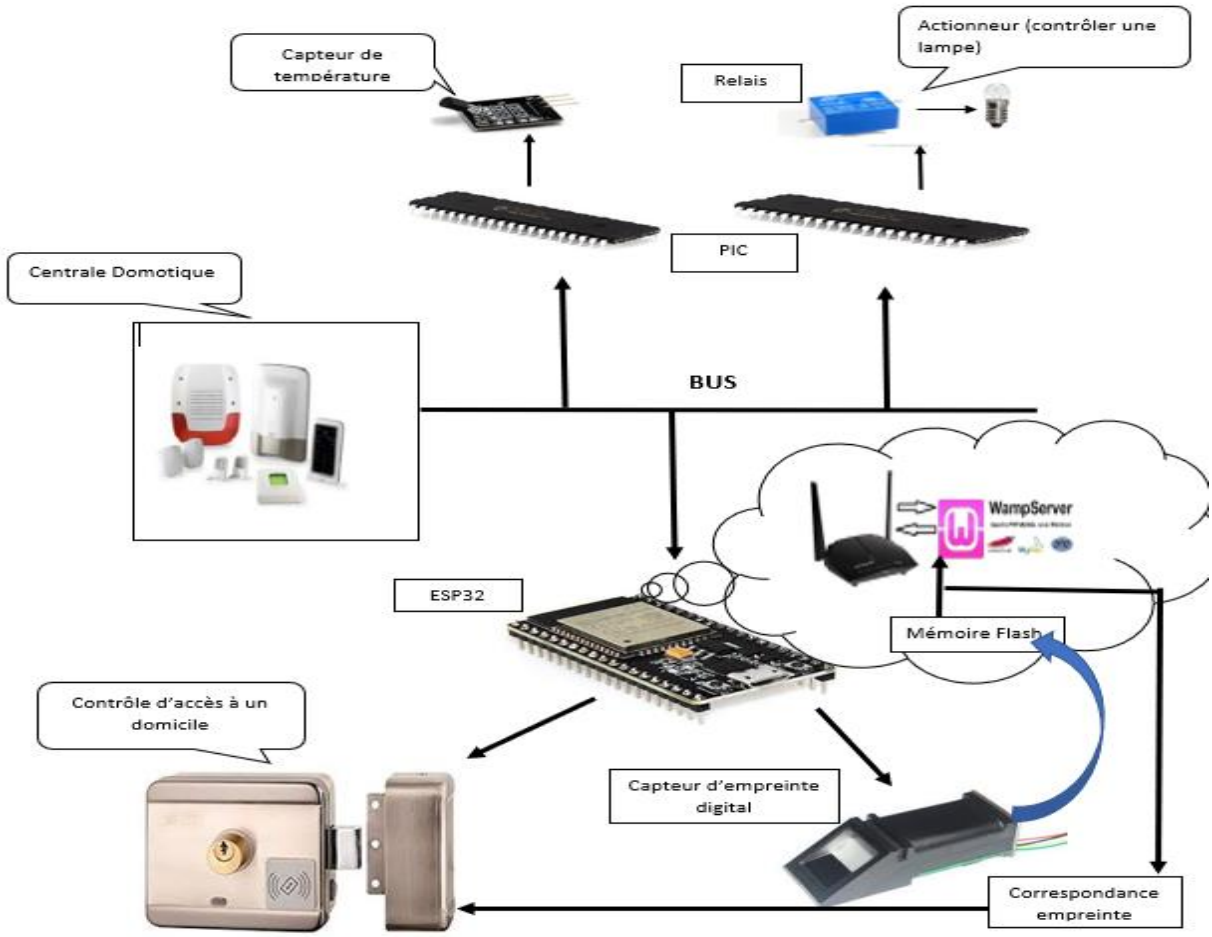


Figure IV.1 : schéma synoptique

Ce système est devisé en deux partie :

- La première partie dispose d'un élément principal qui est la centrale domotique qui initie la conversation avec les équipements (capteurs, actionneurs) à travers le bus I2C. Cette partie est réalisée par d'autres binômes en prenant comme exemple une centrale Google Things à base d'une Raspberry PI et des équipements réalisés à base du microcontrôleur PIC16F877.

  La deuxième partie qui est l'objet de notre travail est le contrôleur d'accès réalisé à base de l'ESP32, du capteur d'empreintes et du mécanisme d'ouverture d'une passe électrique.

IV.3 Conception matérielle

IV.3.1 ESP32-DevKit MH-LIVE [21]

ESP32-DevKit est une carte de développement de petite taille, basée sur ESP32, produite par Espressif. La plupart des broches d'E / S sont réparties sur les en-têtes de broches femelles des deux côtés pour faciliter l'interfaçage. Les développeurs peuvent connecter ces broches aux périphériques en fonction des besoins. Les embases femelles standard facilitent également le développement lorsque vous utilisez des fils Dupont. La carte prend en charge divers modules ESP32, notamment les séries ESP32-WROOM-32, ESP32-WROOM-32U, ESP32-WROOM-32D, ESP32-SOLO-1 et ESP32-WROVER.

FigureIV.2 : carte ESP 32.

IV.3.2 Caractéristiques de la carte

- **Connectivité sans fil**
  - **Wifi** : débit de données de 150,0 Mbps avec HT40
  - **Bluetooth**: BLE (Bluetooth Low Energy) et Bluetooth Classique
- **Processeur** : microprocesseur LX6 32 bits Dual-CoreTensilicaXtensa, fonctionnant à 160 ou 240 MHz
- **ROM** : 448 Ko
- **SRAM** : 520 Ko
- **Basse consommation** : garantis que vous pouvez toujours utiliser les conversions ADC, par exemple pendant le sommeil profond.
- **Entrée / sortie périphérique** :
  - Minuteries et chien de garde
  - Horloge temps réel
  - Convertisseur analogique-numérique (ADC) 12 bits
  - Convertisseur numérique-analogique (DAC)
  - Capteurs intégrés (Température, effet Hall)
  - Détecteur tactile capacitif
  - Co-processor Ultra Low Power (ULP)
  - Interface Ethernet MAC
  - Contrôleur hôte SD / SDIO / MMC
  - Émetteur récepteur universel asynchrone (UART)
  - Interface 2 fils (I2C)
  - Interface son interconnecté intégré (I2S)
  - Interface de périphérique série (SPI)
  - Télécommande infrarouge
  - Compteur d'impulsions
  - Modulation de largeur d'impulsion (PWM) 16 sorties
  - Accélérateur Matériel
- **Sécurité** : accélérateurs matériels pour AES et SSL / TLS

IV.3.3 Capteur d'empreinte FPM10A [22]

Ces modules contiennent une mémoire FLASH pour stocker les empreintes digitales et fonctionne avec n'importe quel microcontrôleur ou système avec liaison série TTL. Ces modules peuvent être ajoutés aux systèmes de sécurité, aux serrures de porte, aux systèmes de pointage du temps, et bien plus encore.

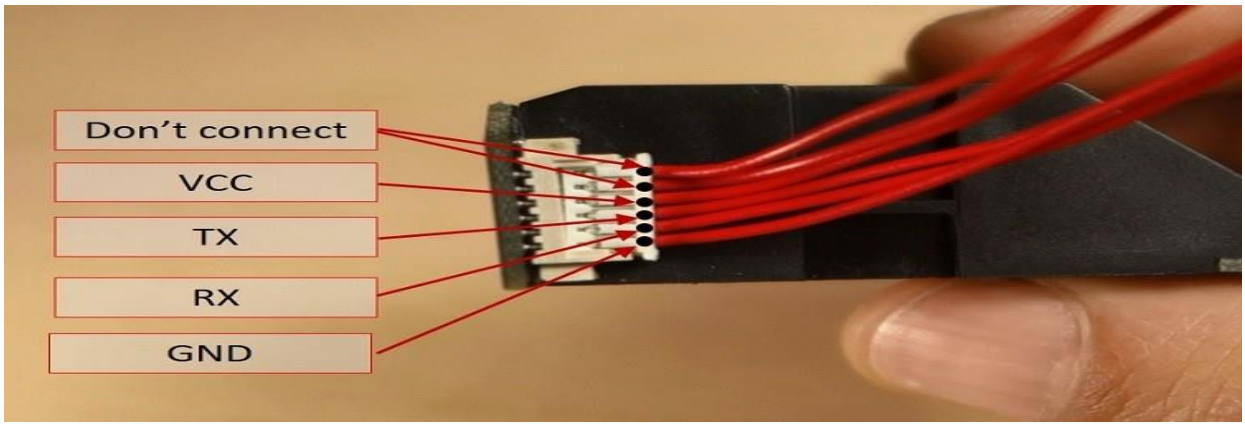
IV.3.3.1 Caractéristiques

- Alimentation en tension : DC 3,6 à 6,0 V
- Alimentation en courant : <120mA
- Couleur de rétroéclairage : vert
- Interface : UART

- Vitesse de communication : 9600 bps
- Niveau de sécurité : cinq (de bas en haut : 1,2,3,4,5)
- Taux de faux positifs (FAR) : <0,001% (niveau de sécurité 3)
- Taux de faux négatifs (FRR) : <1,0% (niveau de sécurité 3)
- Capable de stocker 127 empreintes digitales différentes

Ce capteur est composé de six Broches :

- GND : Masse.
- RX : récepteur.
- TX : Transmetteur.
- VCC : Alimentation.
- T-OUT : pin non connecter.
- DNC : pin non connecter.

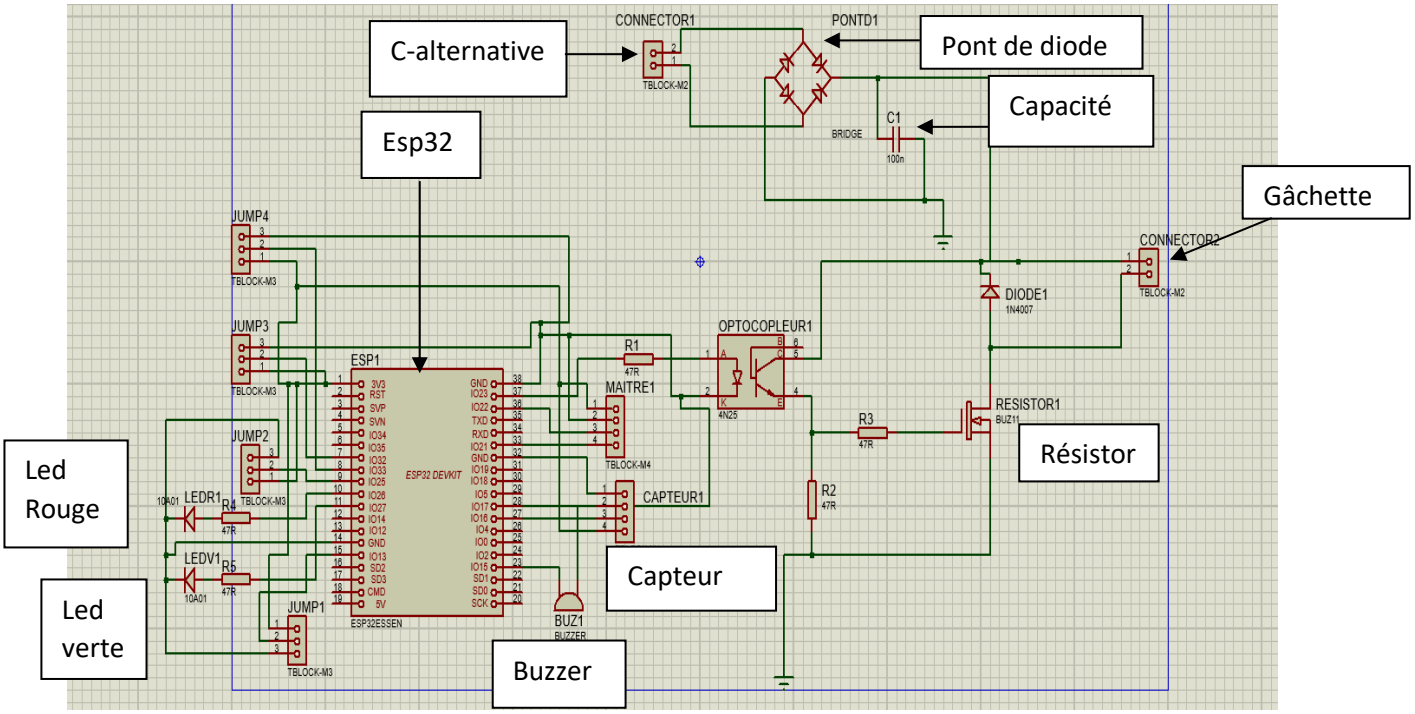


FigureIV.3 : capteur d'empreinte digital.

IV.3.4 Description schématique

IV.3.4.1 Schéma électrique

La FigureVI.4 donne le schéma électrique de notre système :



Figures IV.4 : schéma électrique sur Proteus.

Deux Leds et un Buzzer sont utilisées pour signaler si une personne est autorisée ou non. La led verte reliée à la broche (GPIO27) s'allume quand la personne est autorisée et la porte est ouverte. La led rouge et le buzzer reliés respectivement au broche (GPIO26) et (GPIO15) sont activés quand la personne n'est pas autorisée.

Le jumper 1(GPIO13) est utilisé pour indiquer au microcontrôleur si l'on souhaite enregistrer une empreinte ou contrôler la validité d'une empreinte. Le connecteur (2) est relié à une gâchette qui fonctionne avec 12v DC (courant continue). Pour obtenir ce courant à partir du courant alternatif 220V (connecteur 1) on a réalisé un circuit d'alimentation en courant continu à base d'un pont de diode et d'un condensateur.

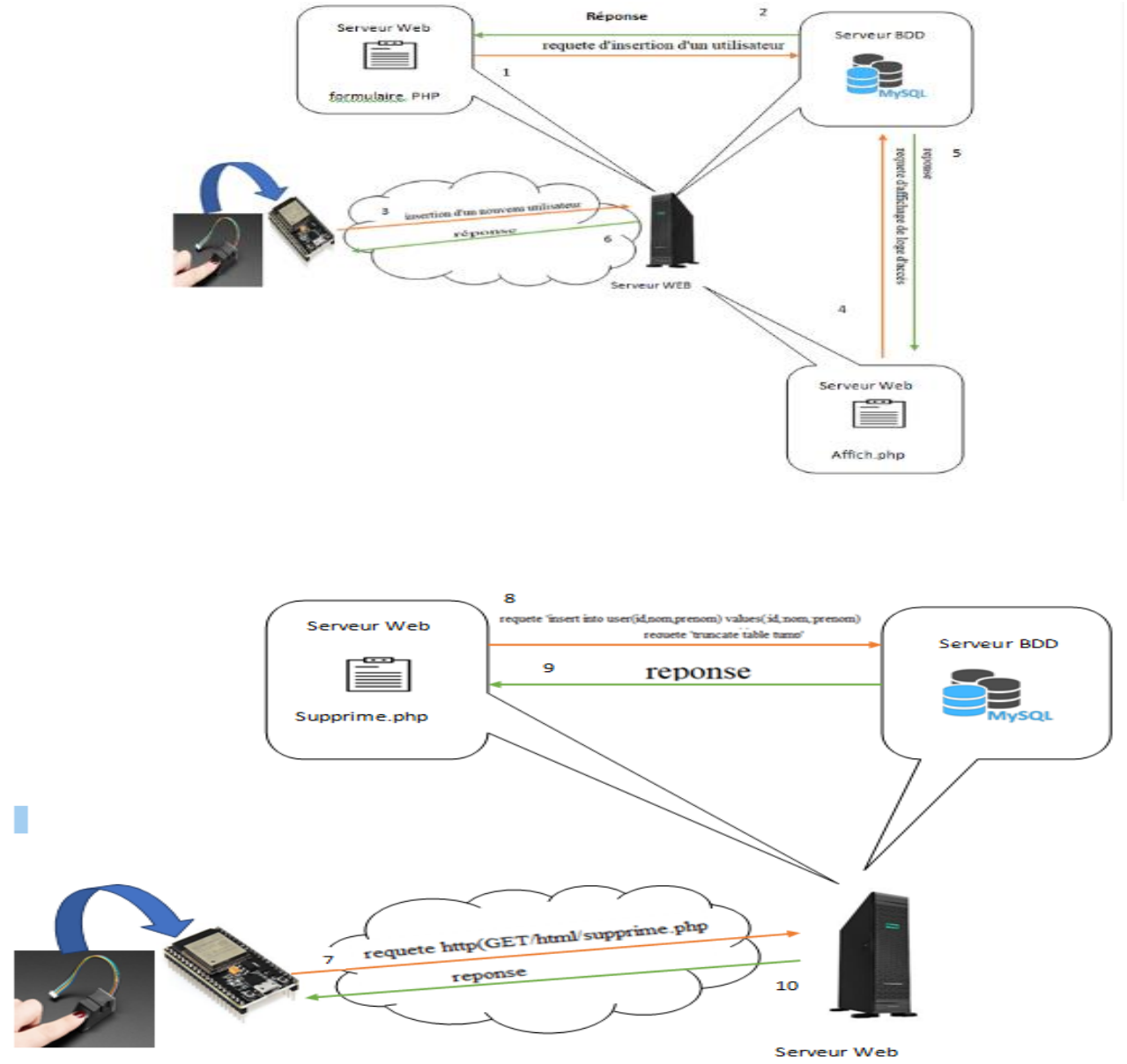
La commande de la gâchette est réalisée en utilisant un optocoupleur permettant de générer un signal 12V quand le microcontrôleur active la broche (GPIO23). Ce signal est ensuite fourni au transistor qui se charge de fournir l'alimentation nécessaire à la gâchette.

Pour spécifier l'adresse de l'esclave au sein de protocole I2C on a utilisé les jumpers (2,3,4), qui sont relié aux GPIO (25, 32,33). La liaison filaire avec la centrale domotique (Le maitre I2C) est effectuée avec le connecteur 3.

IV.4 Conception logicielle

Le logiciel de contrôle de notre système est basé sur deux Phase : enregistrement et contrôle.

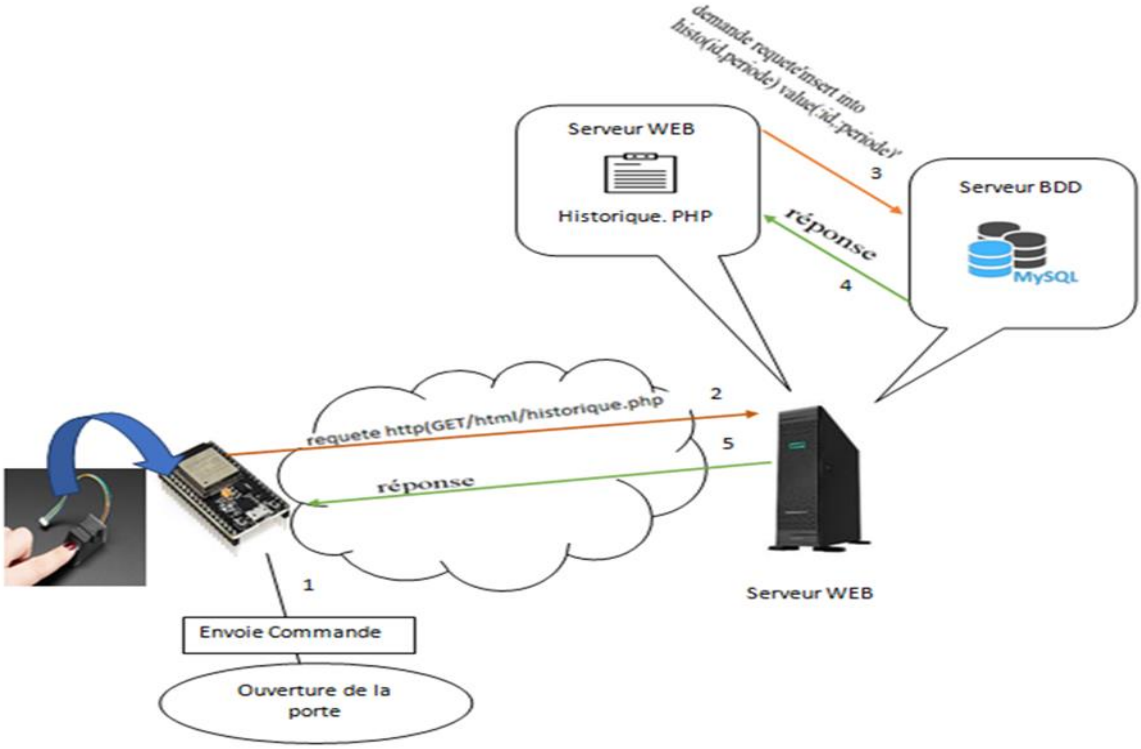
PHASE I :



FigureIV.5 : Schéma Synoptique logiciel ‘phase d’enregistrement’

- La figure IV.5 décrit La phase d'enregistrement d'une empreinte digitale, on commence par accéder à la page web (Formulaire.php) où on doit remplir les informations nécessaires d'une personne (ID, NOM, PRENOM), qui seront stockées dans la base de données (table tump). Quand l'utilisateur sélectionne le mode d'enregistrement sur la carte (à l'aide du jumper 33), l'ESP32 envoie une requête http (GET/HTML/affich.php) au serveur web pour récupérer l'id qui sera associéà l'empreinte et une deuxième requête http (GET/HTML/supprime.php) qui copie les données de la table tump vers la table (user) ensuite les supprimer de la table (tump).

Phase II :



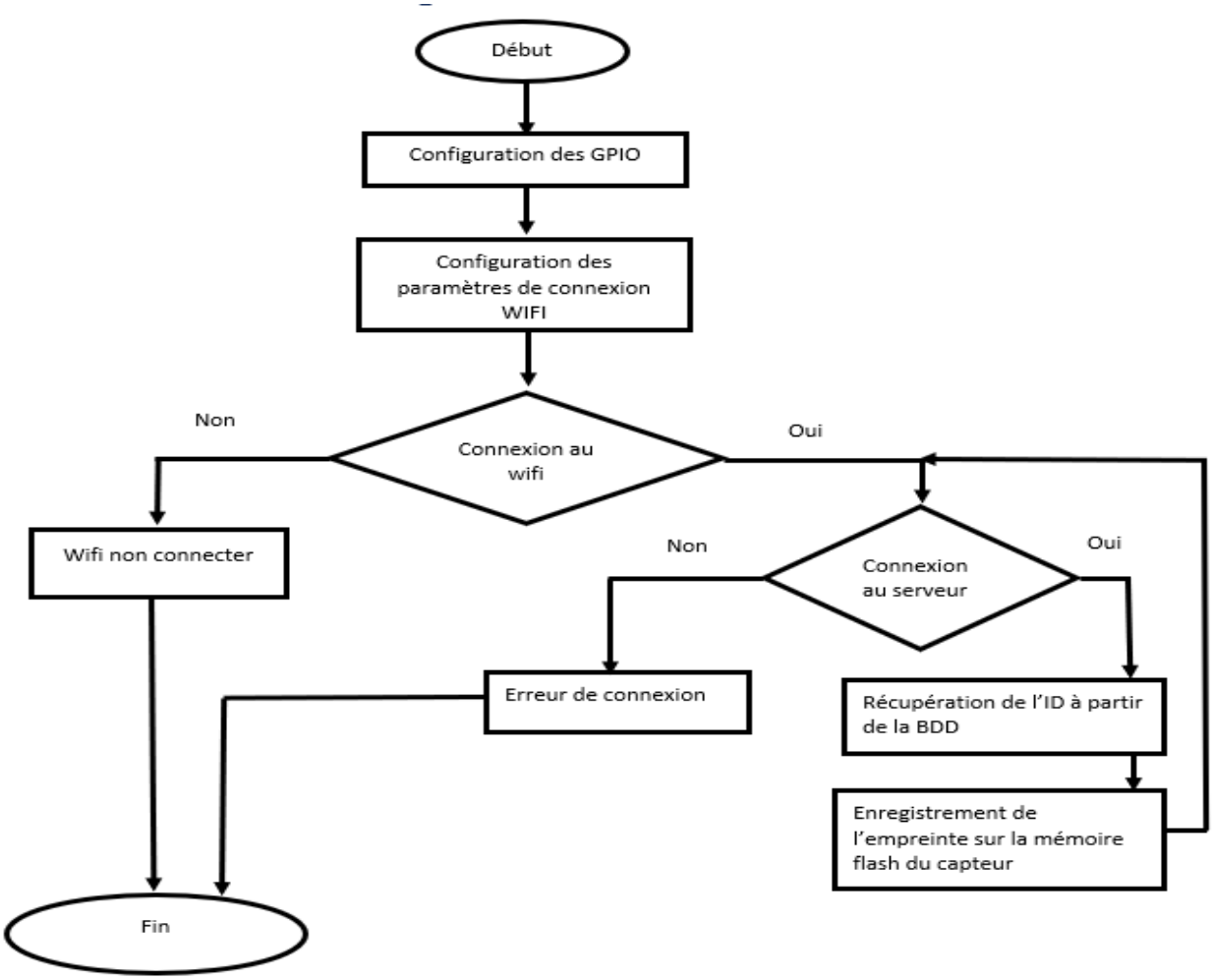
FigureIV.6 : Schéma Synoptique logiciel 'phase de contrôle'

- La figure IV.6 décrit La phase de contrôle d'accès aux utilisateur, L'utilisateur soumet son empreinte au système pour vérification, Si ce dernier est autorisé, une commande d'ouverture est générée, puis une

requête http (GET/HTML/historique.php) est envoyée au serveur web pour enregistrer l'événement.

IV.4.1 Processus de la Phase d'enregistrement

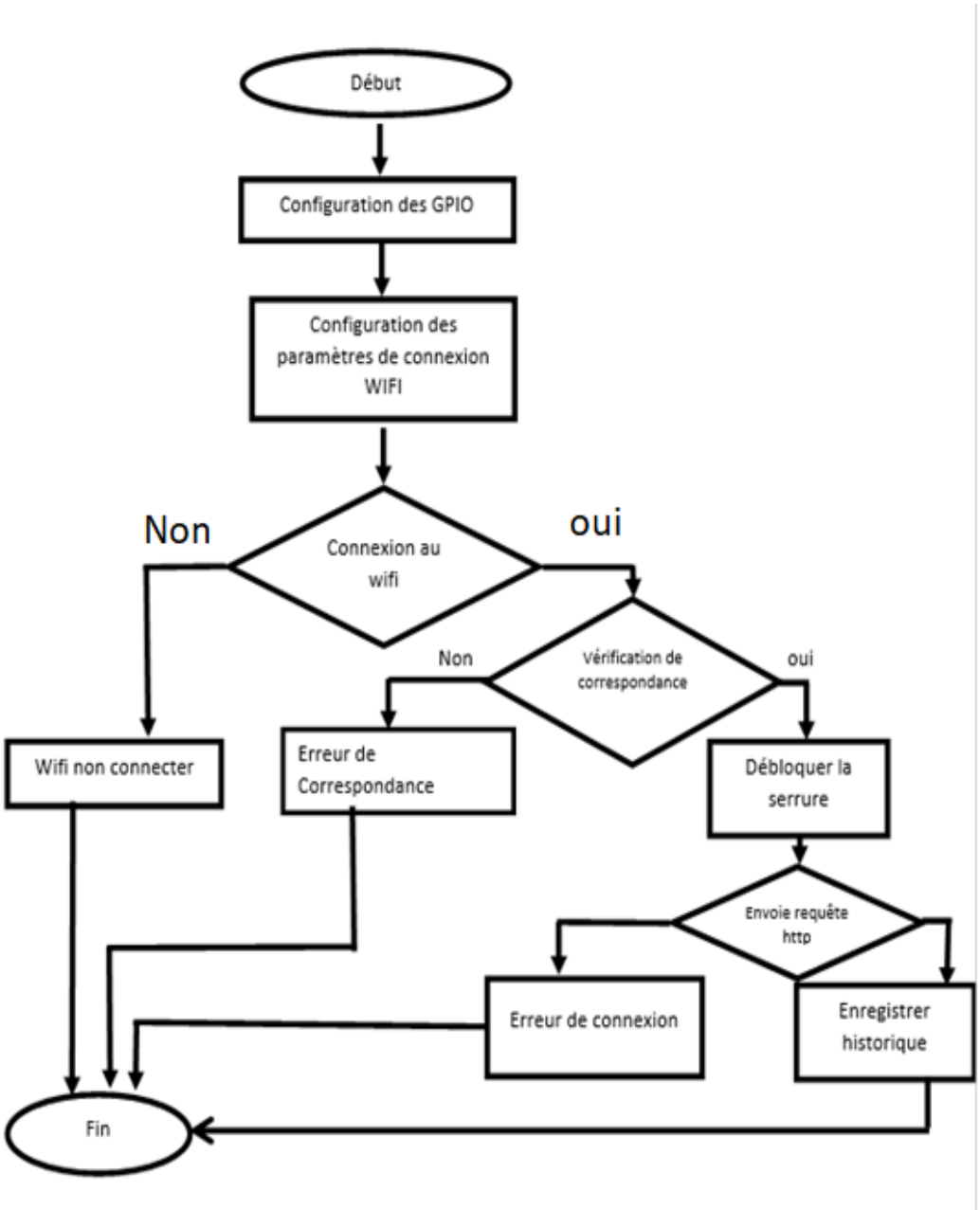
La figure VI.7 Donne l'organigramme de processus d'enregistrement qui décrit son fonctionnement global. En premier temps, on configure les GPIO et paramètres de connexion wifi, ensuite dès que la liaison wifi est établie, on accède au serveur pour récupérer l'id à partir de la base de données qui sera associée à l'empreinte. Ensuite, l'utilisateur est invité à soumettre son empreinte au capteur, une fois l'empreinte capté, elle est enregistrée et associée à l'identificateur introduit



FigureIV.7 : organigramme du programme de la phase enregistrement.

IV.4.1 Processus de la Phase de contrôle

La figure IV.8 Donne l'organigramme du processus de contrôle qui décrit son fonctionnement global. En premier temps, on configure les GPIO et paramètres de connexion wifi, ensuite dès que la liaison wifi est établie, il procède à la comparaison de l'empreinte introduite et celle qui est stockée dans la mémoire flash du capteur, si l'empreinte est valide la serrure sera débloquée, l'esp envoie une requête http pour l'enregistrer dans l'historique.



FigureVI.8 : Organigramme du programme de la phase contrôle.

IV.5 Conclusion

Au cours de ce chapitre, nous avons présenté les différentes étapes constituant le projet. Au début on a commencé par un schéma synoptique qui nous a aidé à comprendre toutes les tâches à accomplir, ensuite nous avons cité les différents composants utilisés, puis on a relié tous ces composants et donné une description schématique du système final.

Finalement, on a présenté la partie logicielle ainsi que les différents organigrammes des processus qui constituent notre application.

Chapitre V

Mise en œuvre

V.1 Introduction :

Après avoir abordé dans le chapitre précédent la conception de notre système, on présente dans ce chapitre les phases de mise en œuvre des différentes parties matérielle et des programmes, ainsi les outils nécessaires à son développement tels que les langages de programmation, et le système de gestion de bases de données utilisés.

Enfin, On présente les principales interfaces via lesquelles les utilisateurs interagissent avec le système.

V.2 Outils utilisés

V.2.1 IDE ARDUINO

V.2.1.1 Introduction

Le logiciel de programmation de la carte Arduino sert d'éditeur de code (langage proche du C) pour notre carte Esp32. Une fois, le programme tapé ou modifié au clavier, il sera transféré et mémorisé dans la mémoire flash de l'ESP à travers de la liaison USB. Le câble USB alimente à la fois en énergie la carte et transporte aussi le programme vers la mémoire flash.

V.2.1.2 Structure générale du programme (IDE Arduino) [23]

L'IDE Arduino est une interface souple et simple, exécutable sur n'importe quel système d'exploitation. Arduino est basé sur la programmation en C.

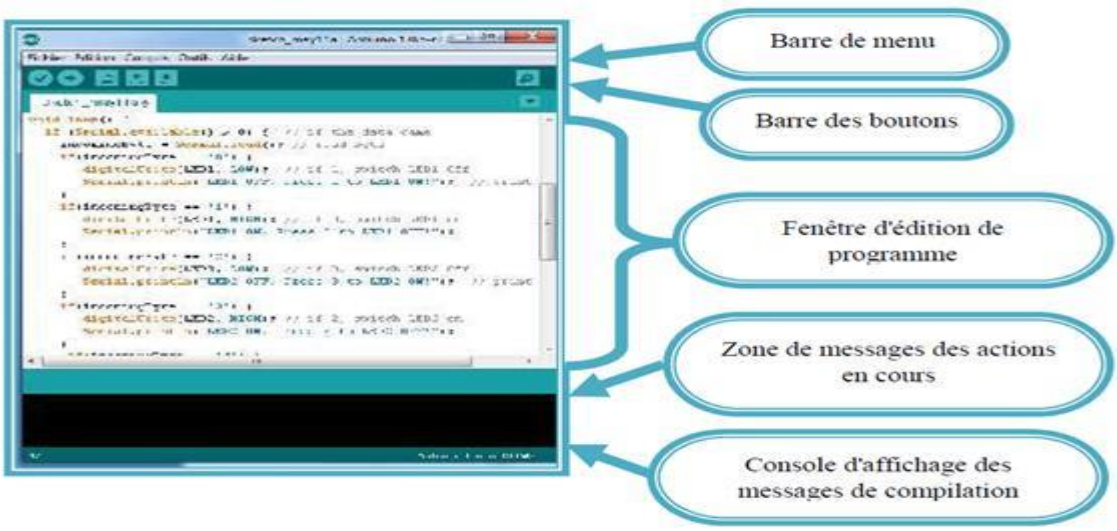


Figure V.1 : Interface IDE Arduino.

V.2.1.3 Injection du programme

Avant d'envoyer un programme dans la carte, il est nécessaire de sélectionner le type de la carte (esp32) [Phase1] et le numéro de port USB (COM 3) [Phase 3] comme à titre d'exemple cette figure suivante.

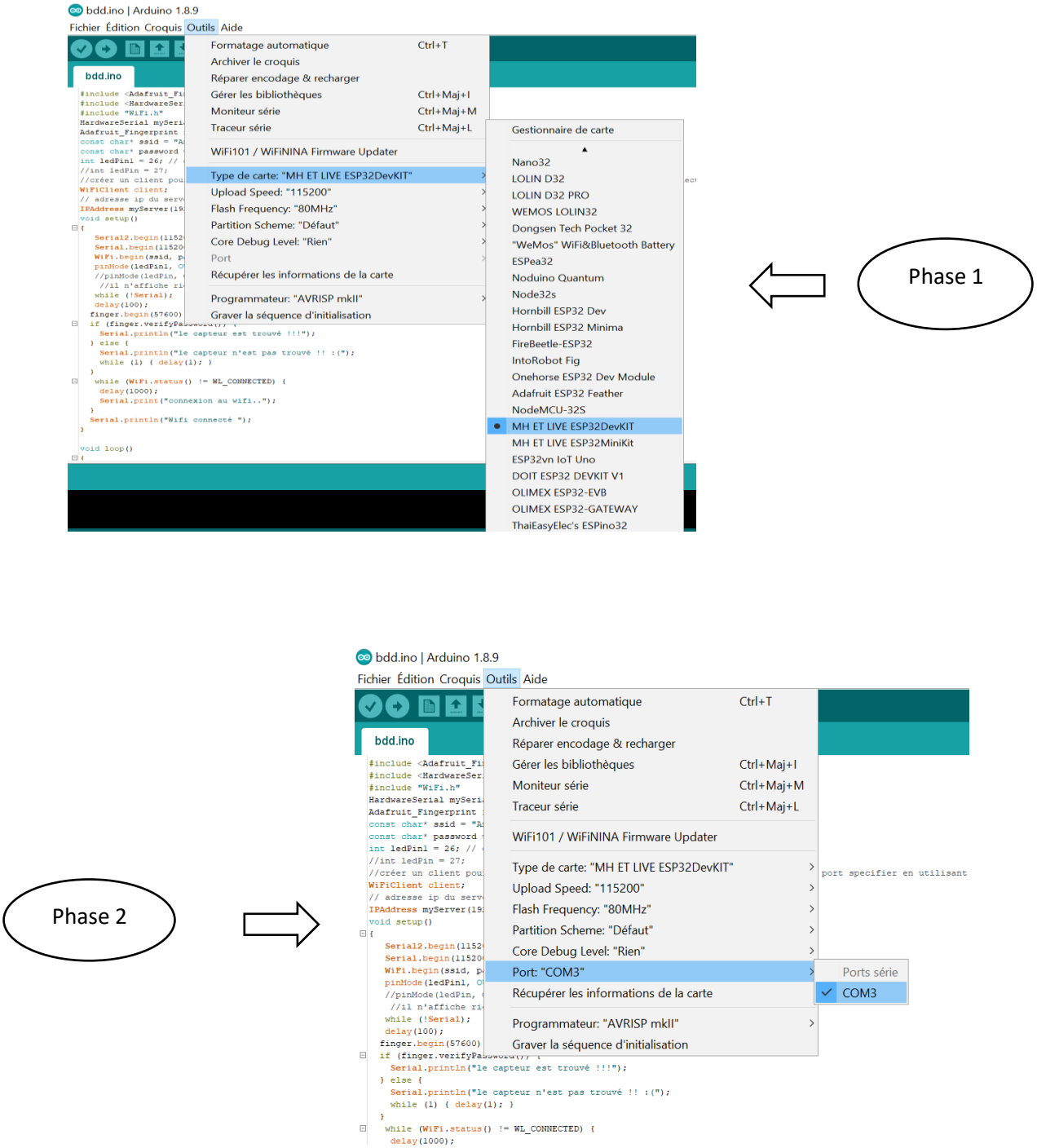


Figure V.2 : Paramétrage de la carte

V.2.1.4 Les étapes de téléchargement du programme

Pour injecter le code on suit les étapes suivantes :

- On écrit ou on ouvre un programme existant avec le logiciel IDE Arduino.
- On compile ce programme avec le logiciel Arduino.
- Si des erreurs sont signalées, on corrige le programme.
- On charge le programme sur la carte.
- L'exécution du programme est automatique après quelques secondes.
- On alimente la carte soit par le port USB, soit par une source d'alimentation autonome (pile 9 volts par exemple).
- On vérifie que notre montage fonctionne.

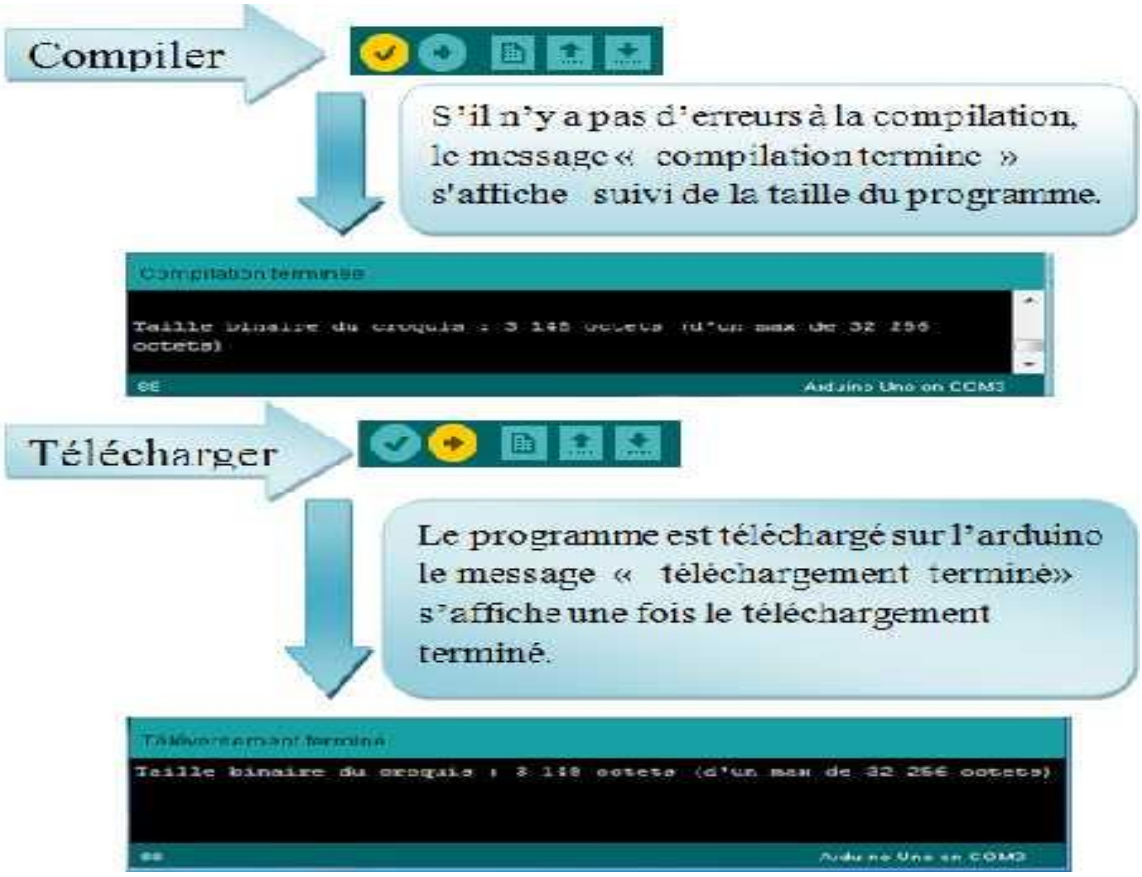


Figure V.3 : Les étapes de téléchargement du code

V.2.2 PROTEUS [24]

PROTEUS est une suite logicielle permettant la conception électronique assistée par ordinateur éditée par la société Labcenter Electronics. Il est composé de deux logiciels principaux : ISIS, permettant entre autres la création de schémas et la simulation électrique, et ARES, dédié à la création de circuits imprimés. Grâce à des modules additionnels, ISIS est également capable de simuler le comportement d'un microcontrôleur (PIC, Atmel, 8051, ARM, HC11...) et son interaction avec les composants qui l'entourent.

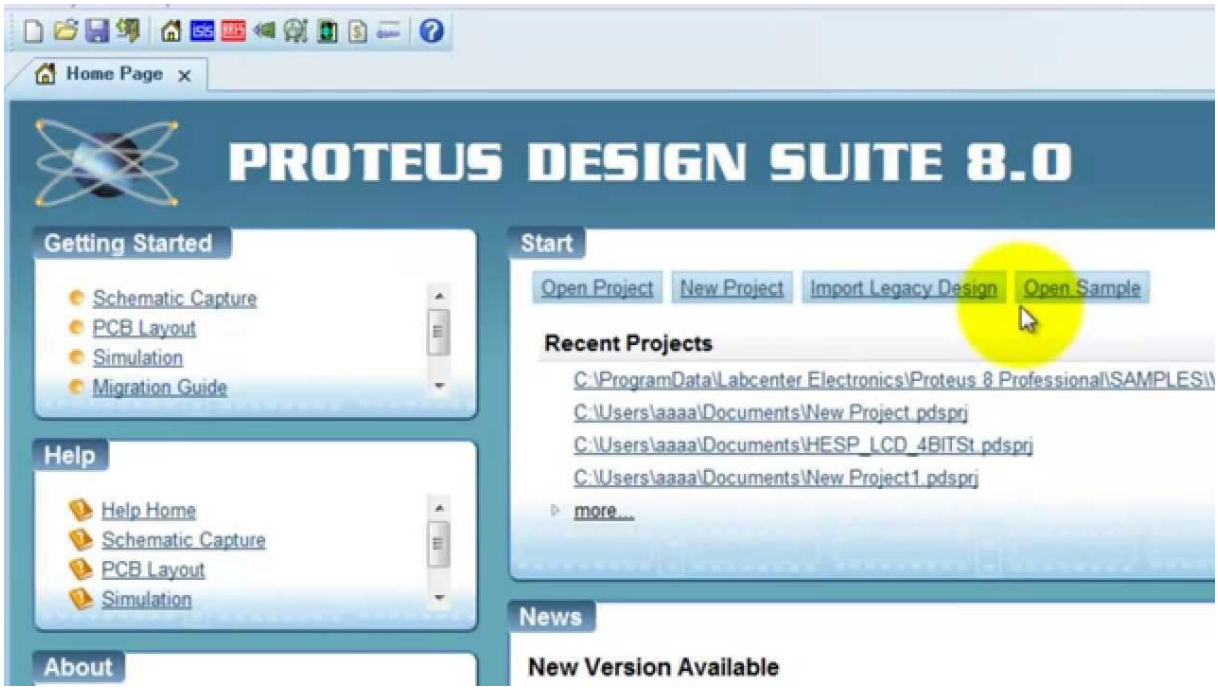


Figure V.4 : logiciel Proteus.

V.2.2.1 ARES [25]

Le logiciel ARES est un outil d'édition et de routage qui complémente parfaitement ISIS. Un schéma électrique réalisé sur ISIS peut alors être importé facilement sur ARES pour réaliser le circuit imprimé de la carte électronique. Ce logiciel permet de placer automatiquement les composants et de réaliser le routage automatiquement.

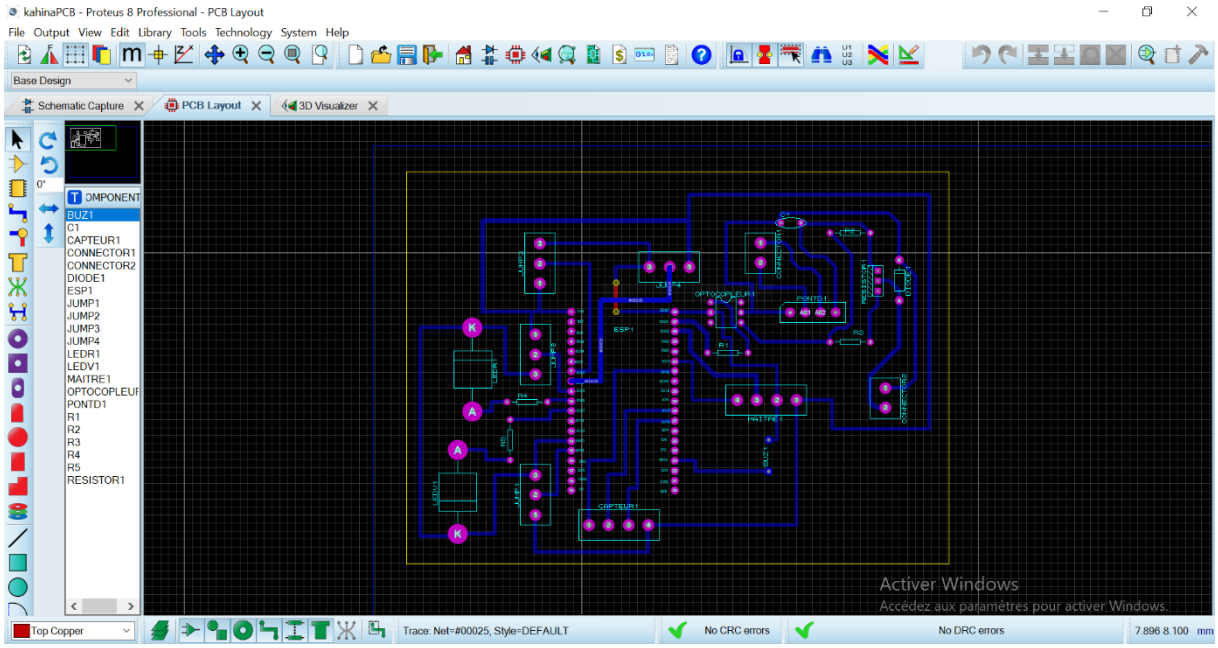


Figure V.5 : Fenêtre principale de travail sur ARES

V.2.2.2 ISIS [26]

Le logiciel ISIS de PROTEUS est principalement connue pour éditer des schémas électriques. Par ailleurs, le logiciel permet également de simuler ces schémas ce qui permet de déceler certaines erreurs dès l'étape de conception. Indirectement, les circuits électriques conçus grâce à ce logiciel peuvent être utilisés dans des documentations car le logiciel permet de contrôler la majorité de l'aspect graphique des circuits.

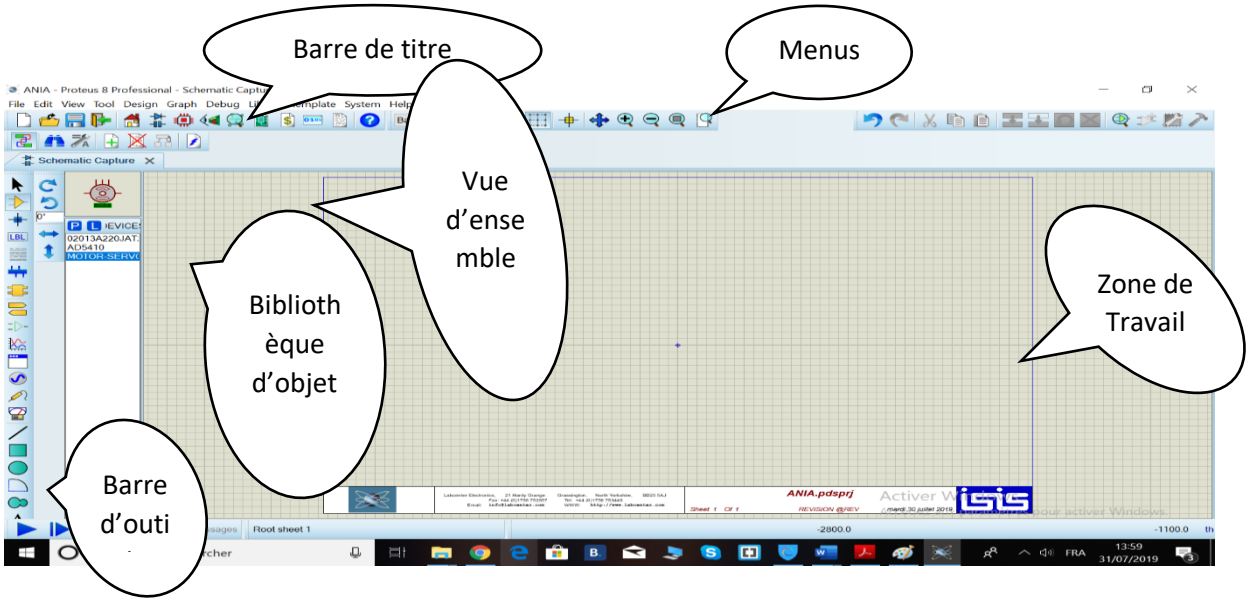


Figure V.6: La fenêtre principale de travail sur ISIS.

V.2.3 WAMP Serveur : [27]

WampServer (anciennement **WAMP5**) est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement (sans avoir à se connecter à un serveur externe) des scripts PHP. WampServer est un environnement comprenant deux serveurs (APACHE et MySQL) un interpréteur de script (PHP), ainsi que phpMyAdmin pour l'administration Web des bases MySQL.

Figure V.7 Serveur wamp.

V.2.3.1 Serveur MySQL

C'est un gestionnaire de base de données relationnelle robuste, basé sur le langage SQL (StructuredQueryLanguage) qui est un langage standard pour le traitement des bases de données. Le serveur MySQL peut fonctionner en mode Client/serveur.

Il contrôle l'accès aux données pour assurer que plusieurs utilisateurs peuvent se servir simultanément d'une même base de données, pour y accéder rapidement et pour garantir que seuls les utilisateurs autorisés peuvent accéder aux données. Le serveur MySQL offre des fonctions nombreuses et puissantes. Ses possibilités de connexion, sa rapidité et sa sécurité font de lui un serveur hautement adapté à internet

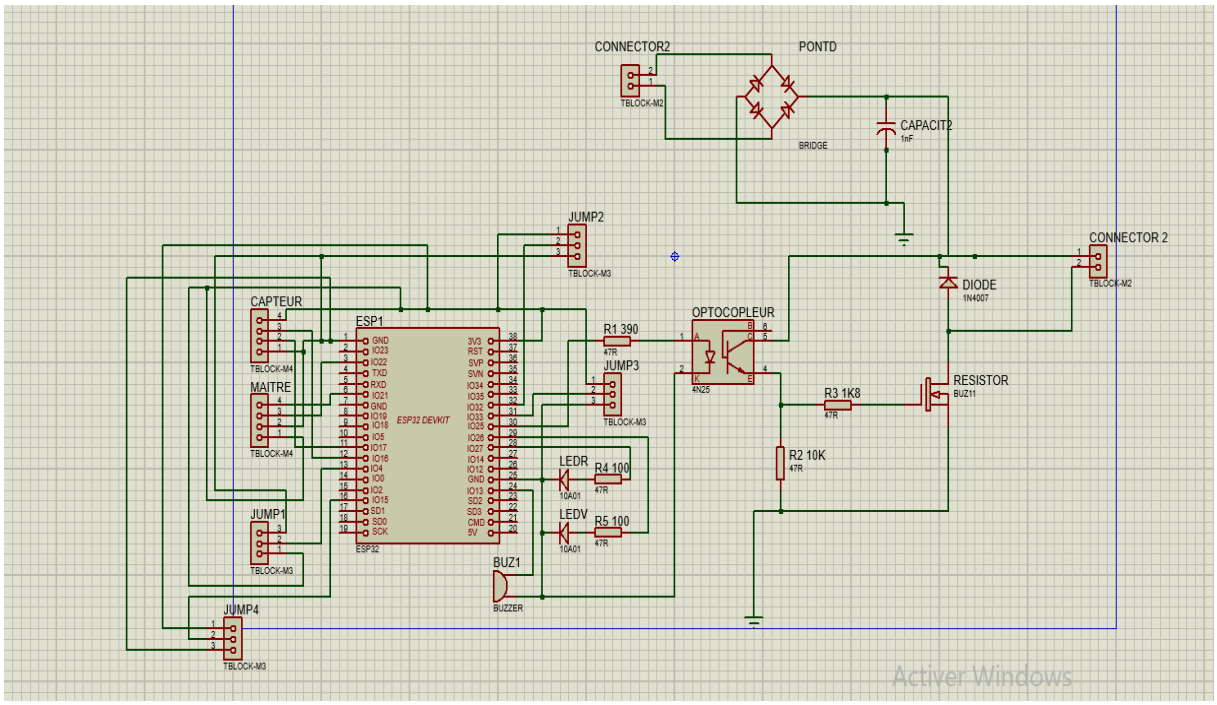
V.2.3.1.1 Serveur Apache

C’est le serveur le plus répandu sur Internet, permettant la configuration de l’environnement d’exécution de pages web. Il s'agit d'une application fonctionnant à la base sur les systèmes d'exploitation de type Unix, mais il a été porté sur de nombreux systèmes, dont Microsoft Windows grâce à sa conception modulaire qui correspond à différents aspects ou fonctions du serveur.

Cette conception autorise le développeur à choisir quelles fonctionnalités seront incluses dans le serveur en sélectionnant les modules à charger soit à la compilation, soit à l'exécution. Elle lui permet aussi d’écrire son propre module qui pourra ensuite être facilement intégré dans le serveur Web Apache.

V.3 Simulation du circuit

Avant de passer au prototype réel il a fallu tester notre système via la simulation et pour cela nous avons utilisé un logiciel



FigureV.8 : simulation de circuit final.

V.4 Circuit final

Pour réaliser le Circuit final il a fallu passer par l'autre partie du logiciel « ISIS » qui est « ARES » ce dernier et conçu spécialement pour la réalisation des « PCB » c'est-à-dire les circuits imprimés.

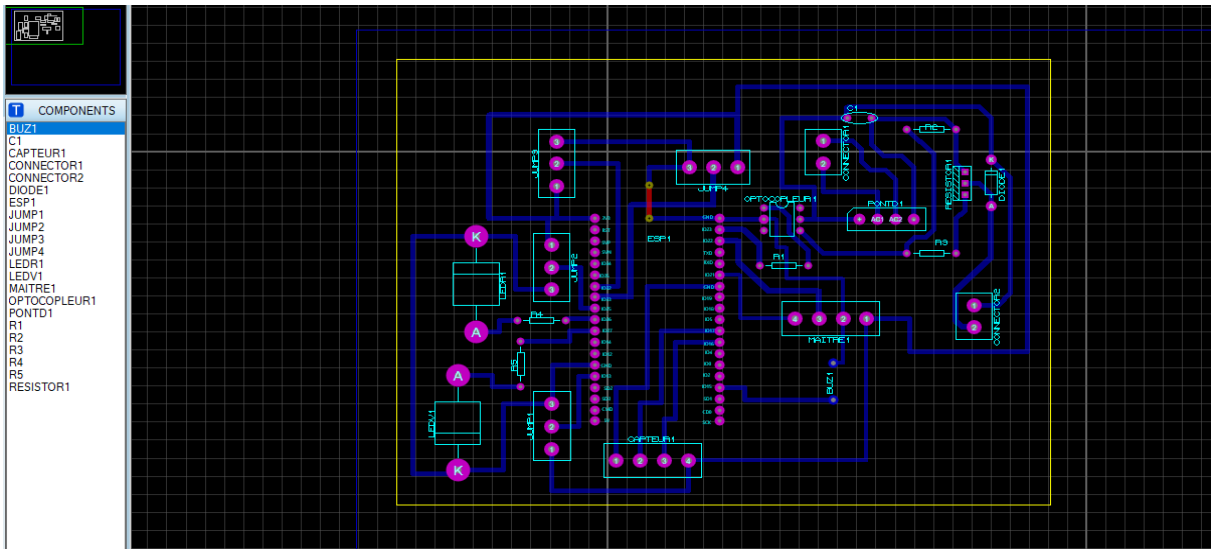


Figure V.9 : Circuit sur ARES.

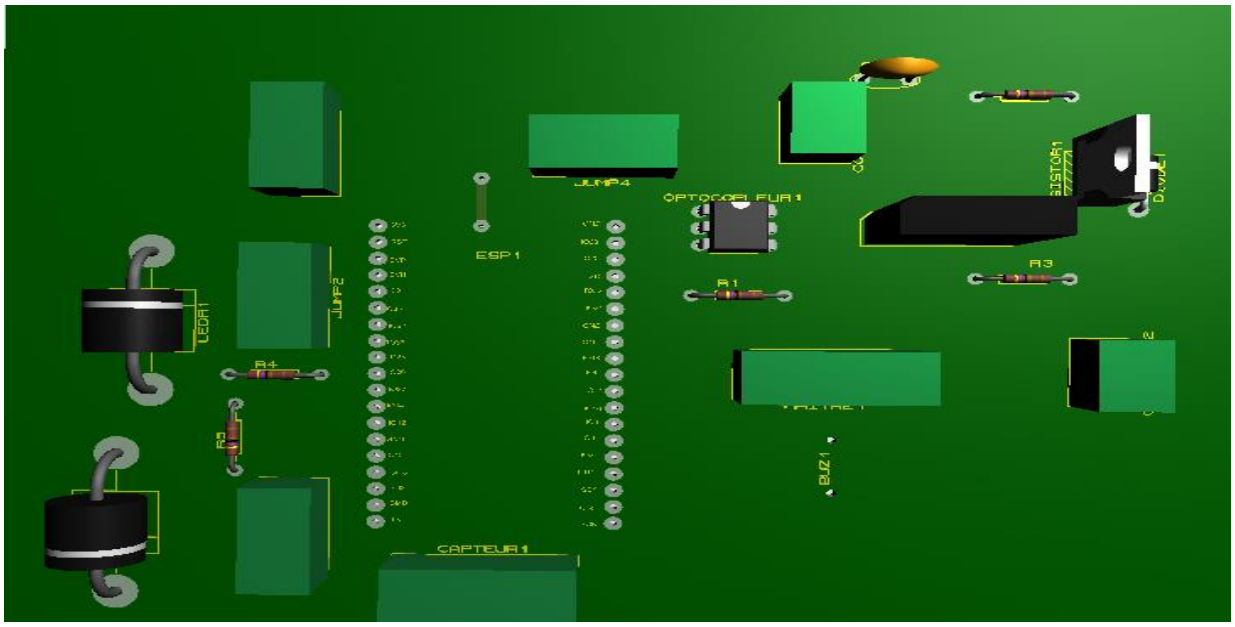


Figure V.10 : Circuit 3D.

V.5 Circuit Imprimé

Nous avons réalisé le circuit imprimé en utilisant la méthode de l'insoleuse (une boite munie de néons), cette méthode consiste à prendre l'époxy et lui coller le typon [Figure V.11], et le mettre dans l'insoleuse pendant trois minutes. Le principe est que les Ultraviolets émis par les néons vont détruire la couche photosensible de l'époxy aux endroits non protégés par le tracé du typon. Une fois le temps écoulé, on sort la plaque pré sensibilisée, on lui retire le typon, puis on la trompe dans une solution révélatrice, puis on la plonge dans un bain de perchlorure de fer en la frottant pour supprimer le cuivre là où il n'y a pas de liaisons. Le résultat Obtenu est montré dans la [figure V.12].

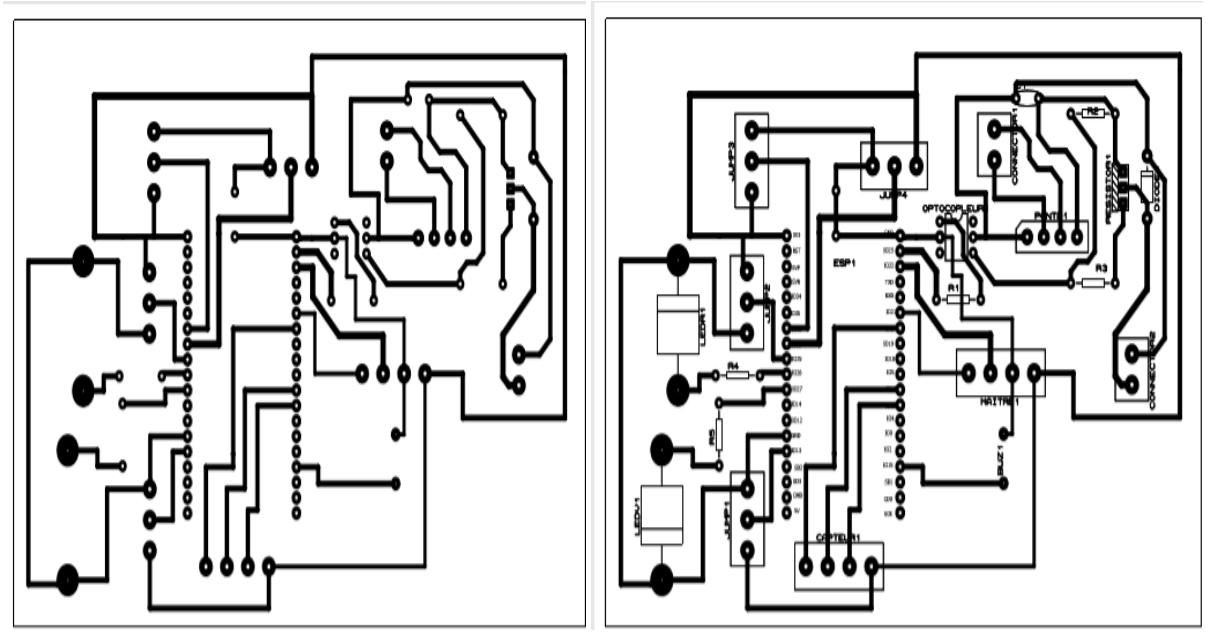


Figure V.11 : Imprimé du circuit ARES sur Du papier Calque (typon).

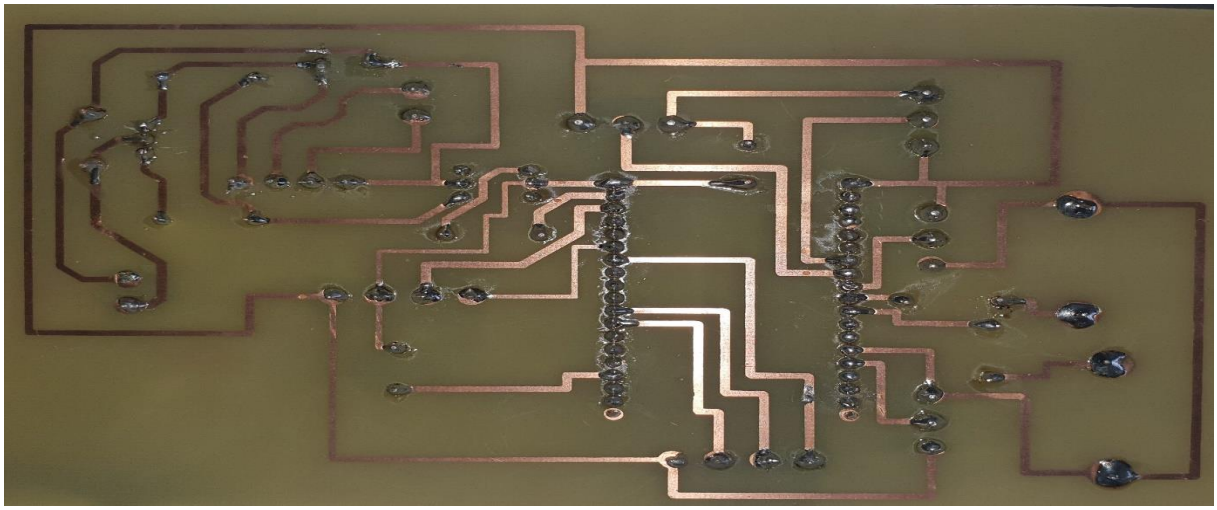


Figure V.12 : Le circuit imprimé de contrôle d'accès.

V.6 Réalisation finale :

Une fois la carte du circuit imprimé est obtenue, une opération « la soudure » est faite après le perforage des Vias où on implante les différents composants sur leurs emplacements [figure V.13].

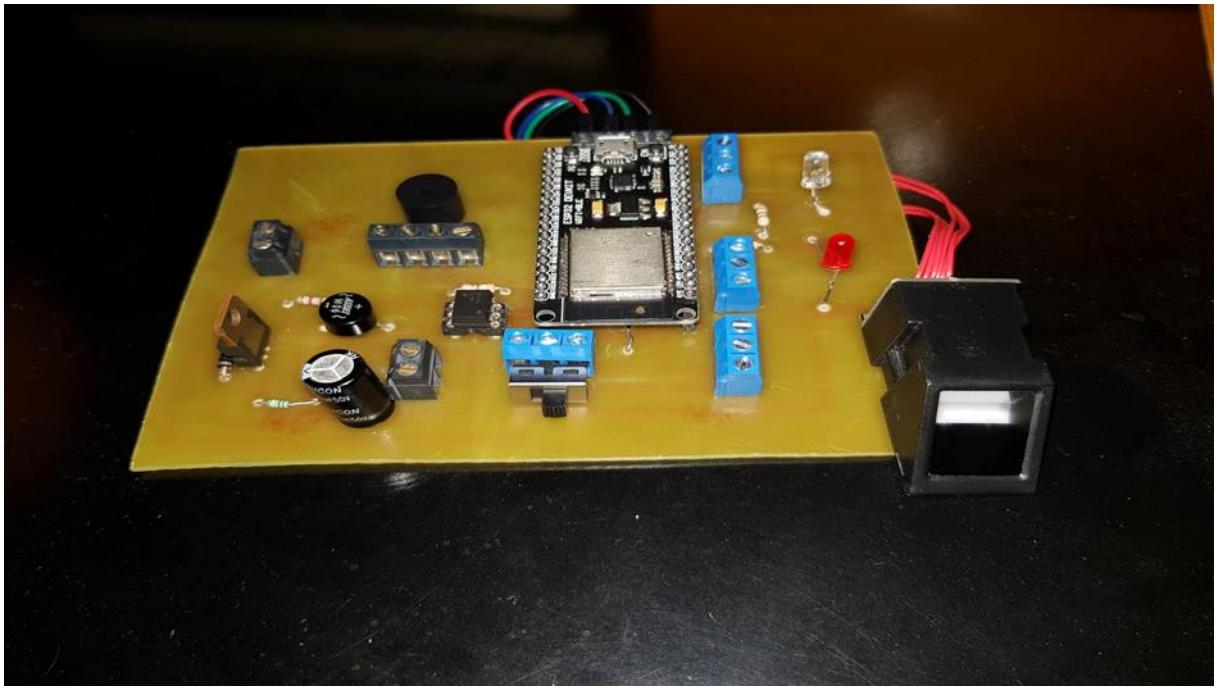


Figure V.13: Circuit final avec les composants.

A la fin, nous avons assemblée la carte précédente, le carte ESP32, La Gâchette avec le boitier d'alimentation. La figure (VI.14) montre la réalisation finale du projet

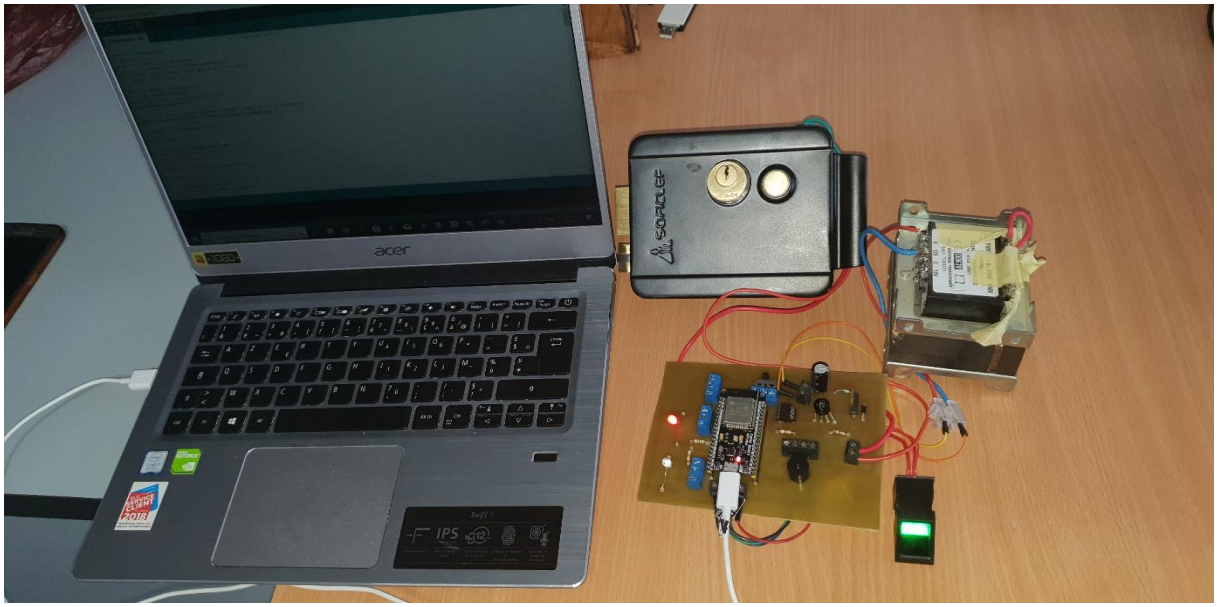


Figure V.14 : La réalisation finale.

Interface d'administration

Cette interface est gérée par l'administrateur où il ajoute des utilisateurs autorisés pour accéder à son domicile.

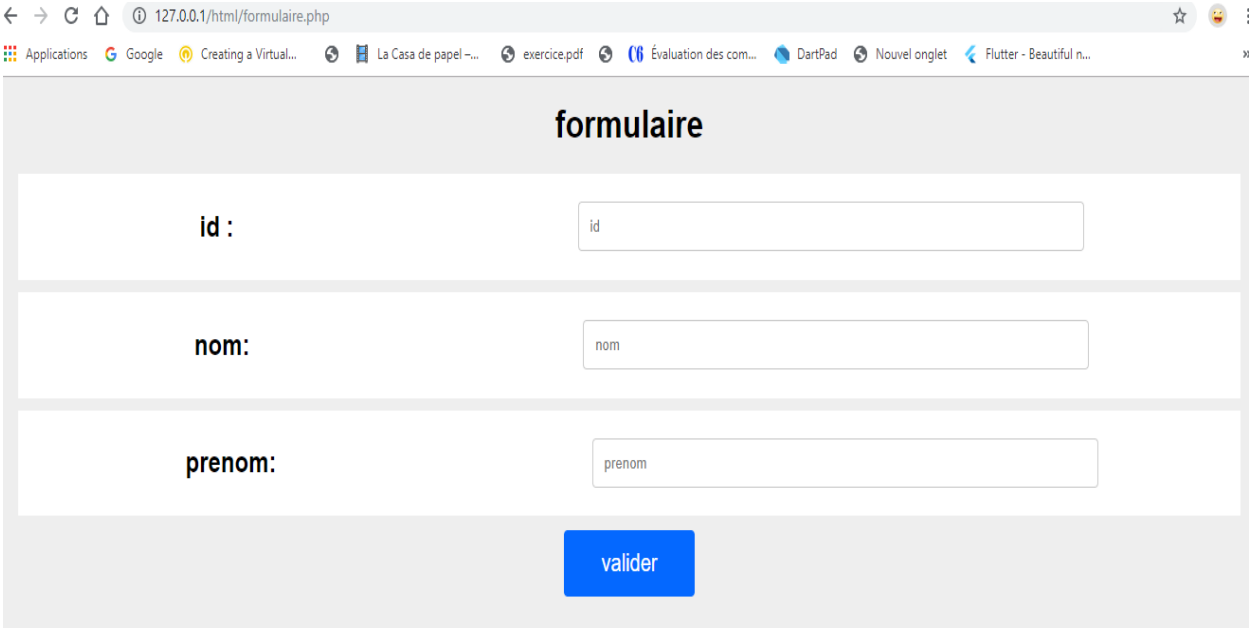


Figure V.15 : Interface 'formulaire d'enregistrement'.

Dans la figure V.16 on a créé une base de données nommée<server>, elle contient 3 tables.

- Table <temp> qui contient trois champ (id,nom,prenom),où l'admin doit remplir tous ses champs pour autoriser un individu à accéder à un domicile .
- Table <user> qui va contenir la copie de la table <temp> après avoir récupérer l'id.
- Table <histo> qui contient deux champ (id,periode) ,utilisé pour enregistrer l'évènement.

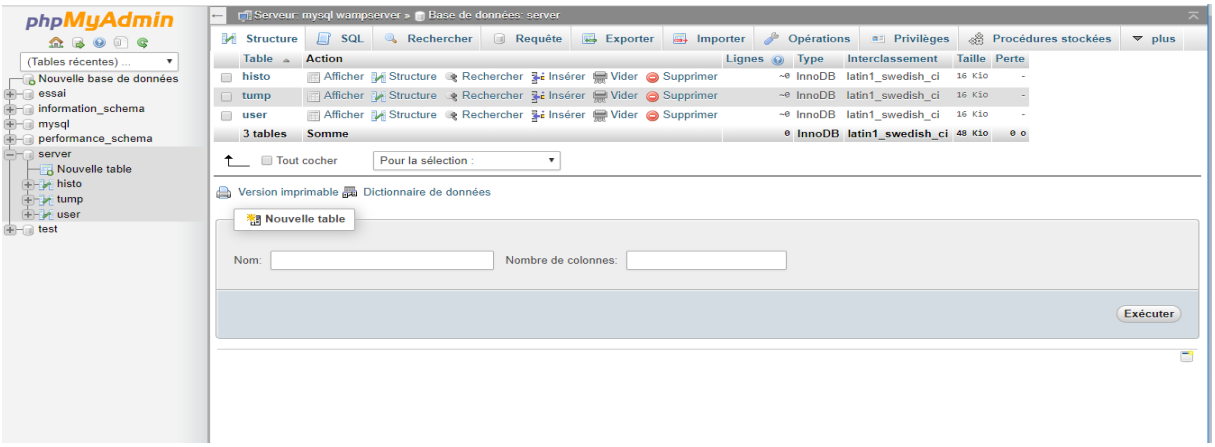


Figure V.16 : Interface des bases de données.

V.7 Conclusion

Dans ce chapitre, nous avons décrit l'aspect pratique de notre projet. On a commencé par présenter les différents outils utilisés, ensuite on a créé un circuit imprimé qui contient tous les composant électroniques qui seront relié au cœur du système (esp 32) et cela grâce au logiciel Proteus, puis nous avons présenté les différentes interfaces de notre projet ainsi que leur comportement.

A travers cette réalisation, nous avons pu atteindre les objectifs fixés lors de la phase de conception.

Conclusion et Perspectives

Conclusion générale :

Notre projet de fin d'étude consiste à concevoir un système de contrôle d'accès permettant l'ouverture automatique d'un accès à un domicile ou à une structure en utilisant l'empreinte digitale des personnes autorisées.

Dans le premier chapitre, nous avons donné une idée globale sur la biométrie, nous avons fait par la suite une étude sur ses différentes techniques.

Pour implémenter notre projet, nous avons utilisée l'une des techniques biométriques la plus employée à travers le monde qui est l'empreinte digitale qui permet de sécuriser l'accès.

Dans le troisième chapitre, on a mis en œuvre une centrale domotique qui initie la conversation avec les équipements (lampe, passe électrique) à travers le bus I2C.

Enfin, nous avons présenté une étude des cas pratique sur toutes les notions théoriques qu'on avons vu dans le chapitre précédent.

En guise de perspectives on envisage d'intégrer ce dispositif dans une station Google Home et ajouter les fonctions nécessaires pour le commander par la voix grâce à Google assistant.

REFERNCES :

[1] Cherifi Nadir Chikhi Massine, Système automatique de reconnaissance faciale, Mémoire de master, 2010 /2011.

[2] Sehad Naima Abdenour Bessah, authentification faciale à base de java Card et GMM, Mémoire de Master,2009/2010

[4] Max Chassé, " La biométrie au Québec : Les enjeux ", Mémoire de Master, Juillet 2002.

[7] Attallah bilal, Conception d'un système de Reconnaissance des empreintes digitales par apprentissage, Mémoire de Master,2012.

[11] & [12] Mostefa Meriem, placement des tâches répétitives sur une architecture régulière embarquée, Mémoire de Master, juin 2009.

[19] bouharaoua abderrahim boukli hacene, automatisation d'une maison intelligente via une application Android, Mémoire de Master,2016/2017.

[23] Krama abdelbasset Gougui abdelmoumen, étude et réalisation d'une carte de contrôle par Arduino via le système Android, Mémoire de Master,2014/2015.

[27] Zerbout Ania Oukil Kahina hami syfax khettab hossamddine, conception et réalisation d'une Application web pour la gestion du document, Mémoire de Licence, 2016/2017.

[3]

Benchennane Ibtissam, Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus, Thèse,

https://www.univusto.dz/images/coursenligne/These_BENCHENNANE_I.pdf.

[5]&[6] Conception et mise en place d'une plateforme de sécurisation par synthèse et reconnaissance,https://www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom3.html.

[10] Les systèmes embarqués,https://www.memoireonline.com/05/12/5830/Les-systemes-embarques.html.

[16] & [17] & [18]

Les protocoles de la smarthome,https://www.trustedreviews.com/opinion/z-wave-zigbee-smart-home-protocols-3426057.

[20] cours systèmes embarqué,https://www.technologuepro.com/cours-systemes-embarques/cours-systemes-embarques-Bus-I2C.htm.

[21] la carte esp32,https://espacerm.com/webgen/2018/11/12/esp32/.

[22] capteur d’empreinte digitale,https://Fingerprint-capteur-dempreinte-digitale-serrures/dp/B07JC2KKRQ.

[24] & [25] & [26] logiciels Proteus, http://elektronique.fr/logiciels/proteus.php.

[8] & [9] http://bib.univoeb.dz:8080/jspui/bitstream/123456789/6791/1/m%C3%A9moire%20pdf.pdf.

[13] & [14] & [15]

http://dspace.univtlemcen.dz/bitstream/112/11548/1/Ms.ELN.Metahri%2BAbdelli.pdf.