REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

AIT AISSA Hana

AOUNE SEGHIR Akram

Filière : Automatique

Spécialité : Automatique et **I**nformatique **I**ndustrielle

---

Conception et réalisation d'un système de pointage à base d'empreinte digitale et de contrôle d'accès par carte RFID.

Soutenu le 03 / 07 / 2024 devant le jury :

GABOUR	Nour el houda	MCB	UMBB	Présidente
GARMAT	Abdelkader	MCB	UMBB	Examinateur
KAOUANE	Mohamed	MCA	UMBB	Rapporteur

Année universitaire : 2023/2024

Dédicaces

Je dédie ce travail :

A mes très chers parents, Que dieu leur donne santé et protection.

A mon rapporteur monsieur KAOUANE.

A ma sœur Sara pour son soutien moral et son mari Nacim avec la petite princesse Ayla Amira.

A monsieur Bilel pour sa patience, madame Cherifa, Asma, Abdou, Salah, Samah, Hayete, Wissem, Melissa et Kahina.

A mes oncles Kheider, Djamel, Mourad et Hakim, à ma tente Sassa.

A mes amis et à tous ceux qui ont été présents pour me soutenir de bon cœur, tous ceux qui me présentent de l'estime et de la considération.

Hana AIT AISSA

Je dédie ce travail :

Premièrement à mes très chers parents. Que dieu leur donne santé et protection.

A mon rapporteur monsieur KAOUANE.

A mon petit frère Achraf, à ma petite sœur Bouchra et Ahlem.

A mes tentes, mes oncles paternelles et maternelles.

A monsieur Bilel, madame Cherifa, Krimou, Aymen, Amdjad, Abdou, Mario, Malek, Abdelmadjid et Salah.

A mes amis et à tous ceux qui ont été présents pour me soutenir de bon cœur, tous ceux qui me présentent de l'estime et de la considération.

Akram AOUNE SEGHIR

Remerciements

On ne remerciera jamais assez Allah le tout puissant pour la volonté, la santé et la détermination dont il nous a doté durant toutes ces longues années de labeur pour notre réussite.

Nous tenons à témoigner notre profonde reconnaissance, et notre gratitude à monsieur KOUANE, notre professeur et rapporteur de ce mémoire, c'est grâce à lui que nous avons enrichi nos connaissances, nous le remercions pour nous avoir témoigné sa patience, sa compréhension, pour l'aide qu'il nous a apporté ainsi que sa grande disponibilité dans le suivi.

Nos remerciements vont aussi à nos enseignants qui ont contribué à notre formation et à tous les membres du jury qui ont accepté de juger notre travail et de notre ténacité.

Hana AIT AISSA et Akram AOUNE SEGHIR

Résumé

L'Empreinte Digitale et la technologie RFID ont chacune une histoire fascinante et ont révolutionné la manière dont nous identifions, sécurisons et gérons les informations. L'Empreinte Digitale, remontant à l'Antiquité, a été utilisée comme moyen d'identification personnelle depuis des siècles, mais ce n'est que récemment, avec l'avènement de la biométrie et des technologies informatiques, qu'elle est devenue un outil central dans les systèmes de sécurité et de gestion d'identité. La carte RFID, quant à elle, trouve ses origines dans les années 1940, mais son utilisation généralisée dans des applications telles que le contrôle d'accès, la gestion des stocks et le suivi des actifs n'a commencé à prendre de l'ampleur que dans les dernières décennies. Ces deux technologies, bien que distinctes dans leur fonctionnement, partagent un objectif commun : simplifier et sécuriser les processus d'identification et de suivi. Dans ce travail, nous réalisons un système, capable premièrement d'identifier les Empreintes Digitales des employés de la Banque pour le pointage des employés, deuxièmement l'accès par la carte RFID pour assurer une sécurité totale à l'aide d'Arduino.

Mots clés : carte RFID, Empreintes Digitales, Arduino.

Abstract

Fingerprinting and RFID technology each have a fascinating history and have revolutionized the way we identify, secure, and manage information. Fingerprinting, dating back to antiquity, has been used as a means of personal identification for centuries, but it is only recently, with the advent of biometrics and computer technologies, that it has become a central tool in security and identity management systems. RFID technology, on the other hand, has its origins in the 1940s, but its widespread use in applications such as access control, inventory management, and asset tracking has only gained momentum in recent decades. These two technologies, although distinct in their operation, share a common goal: to simplify and secure the processes of identification and tracking. In this work : we implement a system capable of firstly identifying employees' Fingerprints for timekeeping purposes, and secondly providing access through RFID cards to ensure total security using Arduino.

Keywords: RFID card, Fingerprints, Arduino.

ملخص

تتمتع كل من تقنية بصمات الأصابع ورقاقات الراديو اللاسلكية بتاريخ رائع وقد أحدثت ثورة في الطريقة التي نحدد بها المعلومات ونؤمنها ونديرها. تم استخدام بصمة الإصبع، التي يعود تاريخها إلى العصور القديمة، كوسيلة لتحديد الهوية الشخصية لعدة قرون، لكنها أصبحت مؤخرًا فقط، مع ظهور القياسات الحيوية وتكنولوجيات الكمبيوتر، أداة مركزية في أنظمة الأمن وإدارة الهوية. من ناحية أخرى، نشأت بطاقة رقاقات الراديو اللاسلكية في الأربعينيات من القرن الماضي، لكن استخدامها الواسع النطاق في تطبيقات مثل التحكم في الوصول وإدارة المخزون وتتبع الأصول بدأ فقط في اكتساب الزخم في العقود الأخيرة. وتشترك هاتان التكنولوجيتان، وإن كانتا متميزتين في تشغيلهما، في هدف م شترك هو: تبسيط .وتأمين عمليتي تحديد الهوية والرصد

في هذا العمل : ندرك نظامًا قادرًا أولاً على تحديد بصمات موظفي البنك لتوجيه الموظفين، وثانيًا الوصول بواسطة بطاقة رقاقات الراديو اللاسلكية لضمان الأمن الكامل باستخدام الاردوينو.

،الكلمات الرئيسية: ، بصمات الأصابع، بطاقة رقاقات الراديو اللاسلكية، الاردوينو.

Table des matières

Liste des abréviations

ADN	l'Acide DésoxyriboNucléique.
APS	Active-Pixel Sensor
CAD	Computer-Aided Design
CCD	Dispositif à Couplage de Charges
CLUSIF	Club de la Sécurité des systèmes d'Information Français
CMOS	Complementary Metal-Oxide-Semiconductor
EEPROM	Electrically Erasable Programmable Read-Only Memory
FBI	Federal Bureau of Investigation
HF	High Frequency
IDE	Integrated Development Environment
IoT	Internet of Things
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
LF	Low Frequency
MINDTCT	Minutiae Detection
MOS	Metal-Oxide-Semiconductor
NIST	National Institute of Standards end Technology
RAM	Random Access Memory
RAND	Research ANd Development
RFID	Radio Frequency Identification
RTC	Real Time Clock
SD	Secure Digital
SPI	Serial Peripheral Interface
UHF	Ultra-High Frequency
UID	Unique IDentifier

Liste des tableaux

Liste des figures

Introduction générale

L'évolution rapide des technologies de sécurité a transformé la gestion des systèmes de pointage et de présence des employés en entreprise. L'intégration de la carte RFID et de l'empreinte digitale s'est imposée comme une solution fiable pour assurer sécurité et précision dans le processus de pointage. Ce mémoire se concentre sur l'étude, la conception et la réalisation d'un système innovant de pointage des employés basé sur ces deux technologies basées sur l'empreinte digitale et carte RFID. En explorant leurs fondements et leurs applications dans le suivi du temps de travail, ce travail vise à améliorer l'efficacité opérationnelle et renforcer la sécurité bancaire. En évaluant les performances et les avantages de ce système, il propose des recommandations pour son déploiement dans divers environnements organisationnels. En combinant la commodité de la carte RFID avec la fiabilité de l'empreinte digitale, cette étude ouvre de nouvelles perspectives dans la gestion du temps et la sécurité bancaire.

Le mémoire se concentre sur la conception d'un système d'accès automatique et sécurisé pour le pointage des employés bancaires. Il est divisé en trois chapitres : une revue des systèmes de pointage existants, une analyse détaillée des composants et des modules utilisés dans la phase de réalisation matérielle, et enfin, la présentation des résultats obtenus.

Chapitre 1

Généralités sur les systèmes de pointage

1.1 Introduction

Le système de pointage est un outil crucial pour la gestion du temps dans les entreprises, surveillant les heures de travail des employés. Son fonctionnement varie selon chaque entreprise et ses objectifs. Il est légalement obligatoire pour les employeurs afin de justifier les heures de travail et éviter les amendes en cas de non-conformité. Les salariés doivent respecter les procédures de pointage, sous peine de sanctions, tandis que les cadres au forfait jours sont évalués sur une base de jours travaillés plutôt que sur des heures spécifiques [1] [2].

1.2 Historique des systèmes de pointage

Les systèmes de pointage ont évolué au fil du temps pour suivre et enregistrer avec précision les heures de travail des employés. Initialement, les méthodes manuelles telles que l'utilisation de feuilles de présence, de cadrans horaires, ou de cartes perforées étaient couramment utilisées. Ces méthodes manuelles étaient souvent sujettes à des erreurs et à des fraudes. Au fil des années, les avancées technologiques ont introduit des systèmes de pointage plus sophistiqués, tels que les pointeuses mécaniques, les pointeuses mobiles, les pointeuses biométriques, et les logiciels de pointage. Les pointeuses mécaniques ont progressivement laissé place à des solutions plus automatisées et numériques, offrant une précision accrue et une gestion simplifiée du temps de travail. Aujourd'hui, les entreprises ont accès à une variété de systèmes de pointage avancés qui intègrent des technologies telles que la biométrie, les applications mobiles, et les logiciels de gestion du temps. Ces systèmes permettent un suivi précis des heures travaillées, la gestion des absences, la planification des équipes, et facilitent la conformité aux réglementations du travail. En résumé, l'évolution des systèmes de pointage a été marquée par le passage des méthodes manuelles traditionnelles à des solutions automatisées et numériques, offrant aux entreprises des outils efficaces pour gérer le temps de travail de manière précise et efficace [3].

1.3 Différents systèmes de pointage

Il existe différents types du système de pointage :

- Pointages manuels ;
- Pointages mécaniques ;
- Pointages électroniques ;
- Pointages informatisés ;
- Pointages biométriques ;

1.3.1 Pointages manuels

Ce sont des systèmes classiques où les employés inscrivent manuellement leurs heures d'arrivée et de départ sur une feuille de présence, un carnet ou un registre.

Figure 1. 1 : Pointage manuel [4].

1.3.2 Pointages mécaniques

Ce sont des dispositifs physiques implantés dans l'entreprise, où les employés utilisent une carte ou un badge magnétique pour enregistrer leur présence. La machine horodatrice imprime ensuite l'heure sur la carte.

Figure 1. 2 : Pointage mécanique [4].

1.3.3 Pointages électroniques

Ils opèrent de manière comparable aux horodateurs traditionnels, cependant, ils emploient des cartes ou des badges pour enregistrer les heures de travail. Les informations sont sauvegardées électroniquement et peuvent être traitées par des systèmes informatiques.

Figure 1. 3 : Pointage électronique par RFID [4].

1.3.4 Pointages informatiques

Ils offrent aux employés la possibilité d'enregistrer leurs heures de travail grâce à un logiciel informatique, qui peut être utilisé sur un ordinateur de bureau, un terminal dédié ou même une application mobile. Les informations sont enregistrées de manière électronique et peuvent être traitées automatiquement.

Figure 1. 4 : Pointage informatisé [4].

1.3.5 Pointages biométriques

Ces systèmes utilisent des caractéristiques physiques uniques de chaque employé, telles que les empreintes digitales, la reconnaissance faciale ou la reconnaissance de la rétine, pour enregistrer les heures de travail. Ils offrent une méthode de pointage précise et difficile à falsifier [2].

1.4 Caractéristiques des différents pointages

Ce tableau ci-dessous représenter les caractéristiques des différents systèmes de pointage.

Tableau 1. 1 : Caractéristiques des systèmes de pointage [2].

Méthodes	Supports	Avantages	Inconvénients
Pointage manuel	Papier (feuille de pointage ou simple feuille de papier).	-Peu coûteuse. - Ne nécessite pas de matériel spécifique.	-Chronophage - Erreurs - Perte des documents. -Consommation élevée de papier. -Difficultés à suivre en temps réel les heures de travail.
Pointage mécanique	Carte	-Précision. -Fiabilité de collecte des données.	-Coût initial élevé - Limité aux sites physiques où les machines sont installées
Pointage électronique	Badge	-Précision. -Traitement et analyse des données. -Suivi en temps reel.	-Coût initial élevé. -Cartes ou badges spécifiques. - Possibilités de perte des badges.
Logiciel	Ordinateur, smartphone	-Flexibilité et facilité d'utilisation -Possibilité d'intégration avec des logiciels RH -Collecte et traitement automatisés des données.	-Connexion internet. -Nécessite un équipement informatique.
Système biométrique	Caractéristiques physiques uniques	-Précision. -Difficile à falsifier. -Pas besoin de badges ou cartes.	-Coût élevé. -Protection de la vie privée des employés. -Possibilités de problèmes de reconnaissance.

1.5 La biométrie

La biométrie est un ensemble de technologies qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, ou la démarche pour différencier des personnes. Cela a été confirmé par Mr Frédéric MASSICOTTE dans sa recherche intitulée 'La biométrie, sa fiabilité et ses impacts sur la pratique de la démocratie libérale « La biométrie est la mesure des caractéristiques physiques d'un individu, que ce soit ses empreintes digitales, la forme de son visage ou encore son ADN » [5].

Selon le CLUSIF « La biométrie est la science qui étudie à l'aide de mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé » [6]. D'après la RAND Public Safety and Justice (Woodward J.D. & al., Biometrics, A Look at Facial Recognition, Documented Briefing prepared for the Virginia State Crime Commission.) « Toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier l'identité qu'un individu affirme » [6].

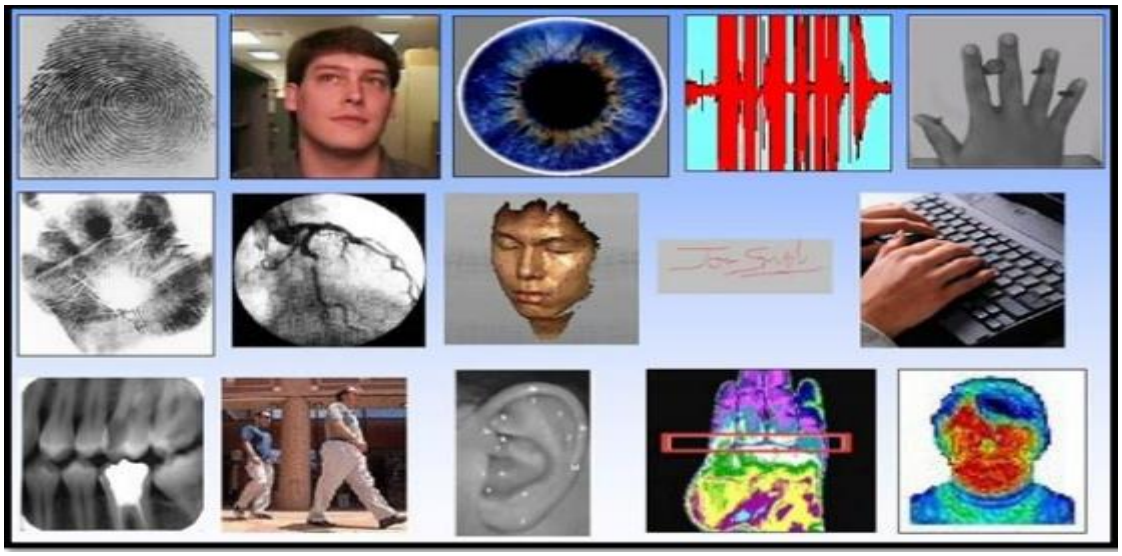


Figure 1. 5 : Différents systèmes biométriques [7].

Un système biométrique est essentiellement une reconnaissance de formes, système qui effectue une identification personnelle en déterminant l'authenticité d'un comportement physiologique ou comportemental spécifique caractéristique possédée par l'utilisateur. Les technologies biométriques doivent idéalement posséder plusieurs caractéristiques [8] :

- **L'unicité :** Cela signifie que chaque attribut biométrique doit varier énormément d'une personne à l'autre.

- **Quanti fiabilité :** Cela signifie que les caractéristiques doivent être mesurées de façon quantitative et leur obtention doit être facile (c'est-à-dire que deux personnes ne peuvent posséder exactement la même caractéristique).
- **L'acceptabilité par la population :** Bien acceptée par les utilisateurs du système.
- **L'universalité :** Toutes les personnes doivent avoir des caractéristiques biométriques.
- **Performances :** L'identification doit être précise et rapide.

1.5.1 Types de biométrie

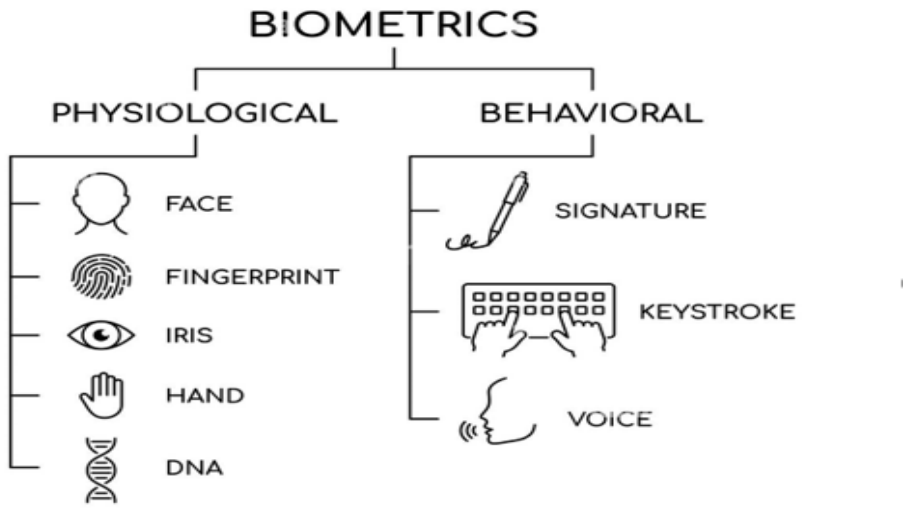


Figure 1. 6 : Types des systèmes biométriques.

1.5.1.1 Analyse physiologique (morphologique)

Cette méthode repose sur la reconnaissance de caractéristiques physiologiques spécifiques qui sont uniques et constantes pour chaque individu. Elle englobe divers éléments tels que l'iris de l'œil, la forme de la main, les empreintes digitales, les caractéristiques du visage, etc.

- **Iris**

L'iris, situé entre la pupille et le blanc de l'œil, présente une structure unique en forme d'anneau, offrant une variété de caractéristiques de texture propres à chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont d'une précision telle que la totalité de la population mondiale pourrait être enregistrée dans une base de données iris avec très peu d'erreurs d'identification. Généralement, l'image de l'iris est capturée à l'aide d'une caméra standard, mais cette étape nécessite la coopération de l'individu. De plus, l'utilisation de cette technologie est soumise à plusieurs contraintes.

Figure 1. 7 : -a) Image d'un Iris-b) Dispositif de reconnaissance de l'Iris [9].

- **Empreinte palmaire**

Cette méthode implique l'analyse de la forme de la main, y compris sa longueur, sa largeur, sa hauteur et la courbure des doigts, entre autres caractéristiques. Elle est relativement récente, simple et largement acceptée par les utilisateurs, qui sont guidés par des indicateurs visuels tels que des LED ou des appareils photo numériques pour positionner correctement leurs doigts. Cela facilite la détection et la segmentation des mains. Cependant, ce type de système peut être trompé par de vrais jumeaux ou des individus ayant des formes de main similaires.

Figure 1. 8 : a) Image de la géométrie de main - b) Dispositif de reconnaissance de la géométrie de main [9].

- **ADN**

L'analyse des empreintes génétiques est une méthode d'identification d'individus extrêmement précise, elle est 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).

Figure 1. 9 : Image de l'ADN [10].

- **Visage**

Les systèmes de reconnaissance faciale actuels se composent d'un module d'acquisition d'images équipé d'une caméra. Initialement, ce module détecte les visages dans l'image acquise. Ensuite, des algorithmes sont utilisés pour traiter l'image et extraire une signature spécifique du visage. Enfin, cette signature est comparée à l'aide d'un classificateur aux signatures déjà enregistrées dans une base de données locale afin d'identifier l'individu [11].

Figure 1. 10 : -a) Image du visage - b) Dispositif de reconnaissance de visage [11].

- **Empreinte digitale**

Les empreintes digitales sont formées par des lignes qui sont localement parallèles et présentent des points singuliers appelés "minuties". Elles représentent un motif distinctif, universel et stable dans le temps. Pour capturer une image des empreintes digitales, des capteurs sont utilisés. Grâce aux progrès technologiques, cette tâche est désormais automatisée à l'aide de capteurs intégrés, éliminant ainsi le besoin traditionnel d'utiliser de l'encre et du papier [11].

Figure 1. 11 : -a) Image d'une Empreinte Digitale - b) Dispositif de reconnaissance d'une empreintes digitales [11].

- **Rétine**

Cette méthode repose sur le schéma et la configuration des vaisseaux sanguins de la rétine, qui sont uniques à chaque individu et relativement stables tout au long de la vie. Bien que très précise, elle est peu répandue et peu acceptée par le grand public et les utilisateurs, car elle nécessite que l'œil soit placé très près de la caméra, généralement à quelques centimètres. Elle est principalement utilisée dans des environnements de haute sécurité, tels que l'accès aux installations nucléaires militaires [12].

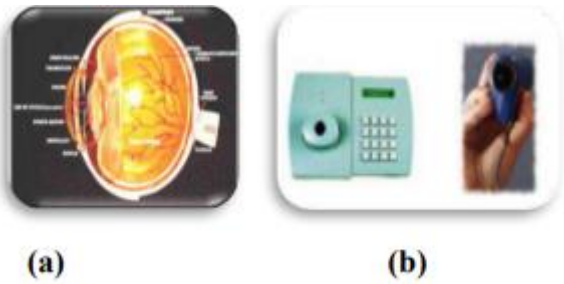


Figure 1. 12 : -a) Image du rétine - b) Dispositif de reconnaissance de rétine [12].

1.5.1.2 Analyse comportementale

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, etc.

- **La reconnaissance vocale**

La biométrie vocale analyse les données provenant à la fois de facteurs physiologiques liés à l'âge, au sexe, à la tonalité et à l'accent, ainsi que de facteurs comportementaux tels que la vitesse et le rythme. Ces caractéristiques sont généralement difficiles à imiter. Actuellement, c'est la seule méthode permettant de reconnaître une personne à distance et elle est généralement bien acceptée par les utilisateurs. Cependant, cette méthode est sujette à des falsifications faciles et nécessite une qualité d'enregistrement excellente. De plus, les différences entre deux voix peuvent être minimes, ce qui rend cette technique peu fiable.

Figure 1. 13 : -a) Image de la voix - b) Dispositif de reconnaissance de la voix [13].

- **La dynamique de frappe au clavier**

Le système repose sur la dynamique de frappe au clavier et ne requiert aucun équipement spécifique, chaque ordinateur étant pourvu d'un clavier standard. Il s'agit d'un logiciel qui enregistre le temps nécessaire à l'appui d'une touche et la période pendant laquelle aucun doigt ne touche le clavier (inter-frappe). Ces données sont enregistrées environ 1000 fois par seconde. Une séquence de frappe est préalablement établie sous forme de mot de passe. L'utilisateur doit initialement entrer son mot de passe à plusieurs reprises afin de créer un modèle de référence.

Figure 1. 14 : Image d'un clavier [10].

- **La signature**

La vérification de la signature examine la manière dont un utilisateur signe son nom, en tenant compte à la fois des caractéristiques dynamiques telles que la vitesse et la pression, ainsi que de la forme géométrique de la signature.

Figure 1. 15 : -a) Image de signature - b) Dispositif de reconnaissance de signature [14].

1.5.2 Biométrie par empreinte digitale

L'empreinte digitale scientifiquement est composée des crêtes qui contiennent des pores et des sillons, et les pores permettent de sortir 80% eaux et 20% matières organiques, ces matières laissent des marques sous formes des lignes [9].

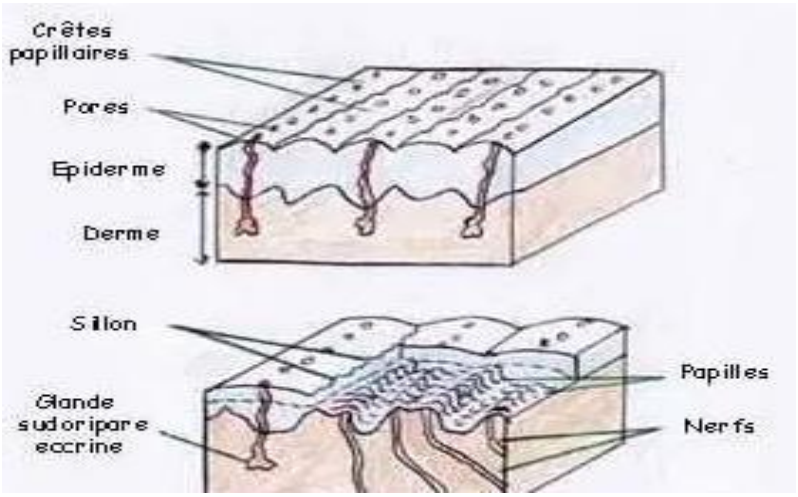


Figure 1. 16 : Etude du dessin digital [16].

1.5.2.1 Historique d'empreinte digitale

L'empreinte digitale a une histoire ancienne, avec des traces découvertes sur des artefacts archéologiques. Cependant, son utilisation à des fins d'identification n'a émergé qu'à la fin du XVIe siècle. En 1864, Nehemiah Grew a réalisé la première étude scientifique détaillée des Empreintes Digitales, jetant ainsi les bases de leur analyse systématique. En 1899, Edward Henry a développé un système de classification des empreintes, marquant une avancée majeure. Au XXe siècle, l'identification par empreintes digitales est devenue courante en médecine légale, avec la création d'agences spécialisées et de bases de données criminelles. Les progrès technologiques ont ensuite permis le développement de techniques de reconnaissance automatique, élargissant leur utilisation à des domaines civils et commerciaux. Aujourd'hui, les empreintes digitales sont largement utilisées dans de nombreux aspects de la vie quotidienne pour l'identification personnelle [17] .

1.5.2.2 Caractéristiques de l'empreinte digitale

Les pointes caractéristiques ou les crêtes sont utilisées pour différencier deux empreintes digitales et aussi faire une classification selon les points singuliers globaux et les points singuliers locaux[17].

- **Les points singuliers globaux**

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

- Le Core : centre ou le noyau contient de courbure maximale des lignes de l'empreinte.
- Le Delta : est proche du lieu où se rencontrent deux lignes, aussi est le lieu de divergence des lignes les plus internes.

Figure 1. 17 : Différentes positions de delta [17].

- **Les points singuliers locaux (minutiers)**

En chaque empreinte il y a des minuties spécifiques permettent de différencier et classer les empreintes, et il y a plusieurs formes des minutiers généralement on a quatre types :

- Les divisions : Bifurcation à droite ou à gauche, intersection de deux stries.
- Les anneaux : Lac, assimilée à deux bifurcations.
- Les coupures : terminaison à droite ou à gauche, minuties situées en fin de celles-ci.
- Les ilots : assimilés à deux terminaisons.

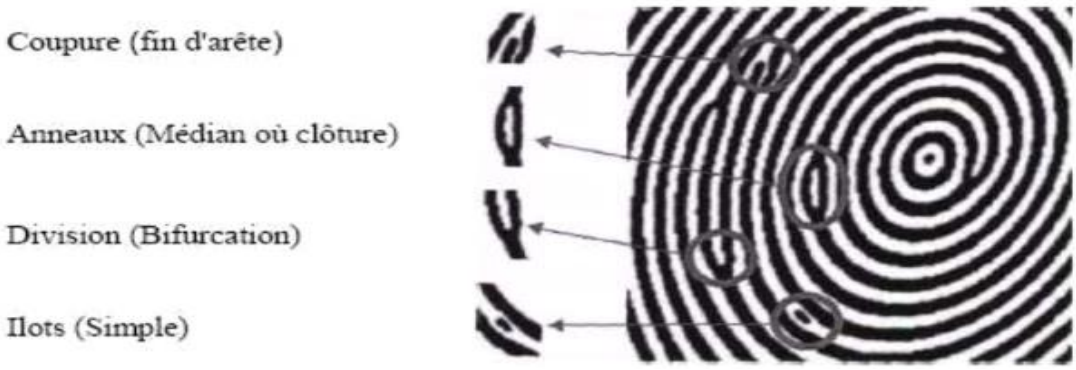


Figure 1. 18 : Les points singuliers locaux [18].

1.5.2.3 Principe de fonctionnement d'empreinte digitale

Un système automatique de vérification (authentification) d'empreintes digitales est une chaîne de traitement qui se scinde en deux étapes : l'enrôlement ou enregistrement et l'authentification comme le présente la figure ci-dessus.

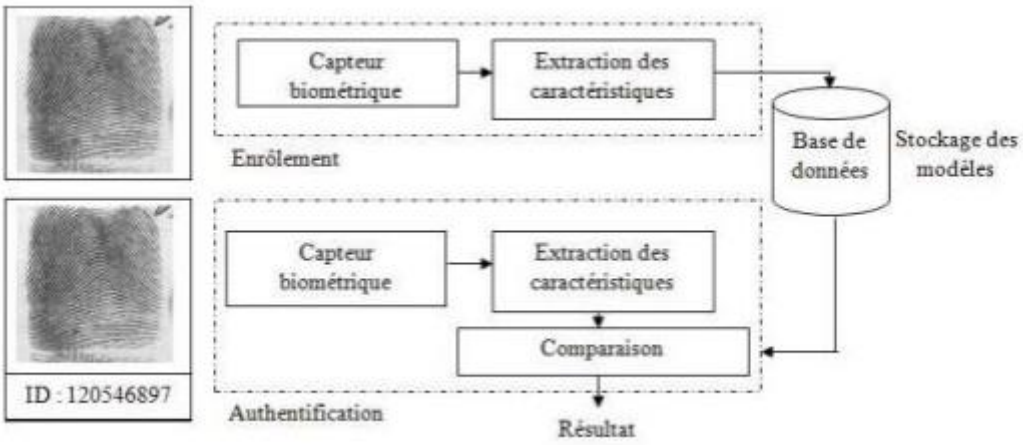


Figure 1. 19 : Architecture d'un système d'authentification par empreinte digitale [19].

Durant l'enrôlement, le trait biométrique de l'utilisateur est capturé (acquisition) et les caractéristiques sont extraites puis sauvegardées dans une base de données comme modèle de référence. Durant l'authentification, le même trait biométrique de l'utilisateur est de nouveau capturé et les caractéristiques sont extraites ensuite comparées avec celles dans la base de données pour calculer leur correspondance.

♣ La phase de capture : Le but de cette étape est de former l'échantillon biométrique sous la forme d'une image numérique en utilisant un dispositif spécial appelé capteur. Aujourd'hui, bon nombre de capteurs d'empreintes existent. Ils se distinguent, notamment par : leur technologie, leur coût, leur qualité d'acquisition, leur facilité d'intégration (téléphone, ordinateur portable) ou leur capacité à détourner les moulages d'empreintes.

♣ La phase d'extraction des caractéristiques : Une empreinte apparaît comme une surface alternée de crêtes et de vallées parallèles sur la plupart des régions. Différentes caractéristiques permanentes ou semi-permanentes telles que les blessures ou les coupures sont aussi présentes sur l'empreinte. Il est nécessaire de définir une représentation invariante appelée gabarit ou modèle. Cette représentation peut être globale prenant en compte toute l'image ou, locale c'est-à-dire constituée d'un ensemble de composantes dérivées chacune d'une région restreinte sur l'empreinte. Le processus usuel d'extraction des minuties se présente comme suit [19] :

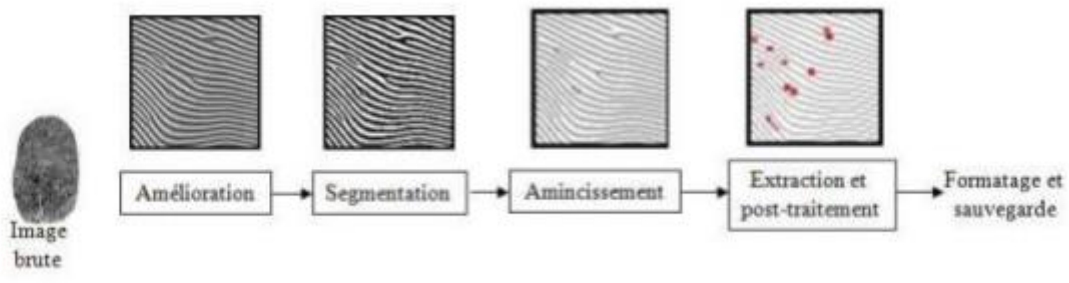


Figure 1. 20 : Processus usuel d'extraction des minuties [19].

Les différentes étapes de la figure 20 sont résumées ci-dessous :

- **Amélioration :** le but de cette étape est d'améliorer la qualité des régions récupérables dans l'image.
- **Segmentation :** l'image en niveaux de gris est convertie en image binaire pour distinguer les crêtes des vallées. Généralement, cette étape fournit de bons résultats à condition qu'elle soit appliquée à des images de bonne qualité ou après une phase d'amélioration.
- **Amincissement :** l'image binaire est soumise à une étape d'amincissement. Quelques algorithmes comme le MINDTCT développé par le NIST pour le FBI ne requièrent pas cette étape.
- **Extraction et post-traitement :** un simple calcul du nombre de connexions d'un pixel crête sur l'image amincie peut informer si le pixel concerné est une minutie ou non. Un post-traitement s'avère toujours utile pour éliminer les fausses alarmes.
- **Formatage et sauvegarde :** les minuties requièrent une représentation très compacte. Chaque minutie peut être décrite par un nombre d'attributs telles que la position, l'orientation et d'autres informations susceptibles d'aider à l'appariement comme son type. Cependant, la plupart des algorithmes considèrent seulement sa position et son orientation.
- **La phase de comparaison :** la mise en correspondance entre deux images d'empreintes diffère suivant la représentation sélectionnée : image, minuties ou descripteur de crêtes, singularités [19].

1.5.3 Technologie RFID

La technologie RFID est un système permettant l'identification et la communication à distance. Elle repose sur l'utilisation d'ondes radio pour transférer des données depuis une étiquette électronique, appelée tag ou carte RFID, qui est attachée à un objet, vers un lecteur. L'objectif est d'identifier et de surveiller l'objet en question. Cette technologie est décrite par Monsieur Calais dans son livre sur les RFID comme étant capable d'identifier un objet équipé d'une étiquette et d'émettre des données via des

ondes radio, et selon Dat Son Nguyen, elle peut fonctionner sans ligne de vue directe et traverser des matériaux fins comme la peinture ou la neige [20] [21].

Monsieur Pierre Georget, quant à lui, détaille la technologie RFID dans son ouvrage « L'identification par Radio Fréquence, principes et application », en la décrivant comme un système déjà largement utilisé pour reconnaître ou identifier à différentes distances, allant du contact à plusieurs mètres, un objet, un animal ou une personne équipée d'une étiquette émettant des données via les ondes radio [22].

Figure 1. 21 : symbole de la RFID [23].

1.5.3.1Historique de technologie RFID

La technologie RFID, abréviation de Radio Frequency Identification, possède une histoire remontant aux années 1940 et 1950. À ses débuts rudimentaires, elle a progressé dans les années 1960 et 1970 avec des systèmes plus avancés utilisant des tags électroniques et des lecteurs pour la lecture à distance. Dans les décennies suivantes, elle a été largement adoptée dans l'industrie pour le suivi des marchandises et la gestion des stocks. Au fil des années 2000, son accessibilité s'est accrue en s'intégrant à diverses applications comme les paiements sans contact et les cartes d'accès sécurisé. Dans la décennie actuelle, elle s'est associée à l'Internet des objets (IoT), permettant le développement d'applications avancées telles que la gestion intelligente des villes. Aujourd'hui, la RFID continue sa progression en intégrant de nouvelles technologies comme l'intelligence artificielle et le « cloud computing, » ouvrant ainsi de nouvelles perspectives dans divers secteurs [24].

1.5.3.2Caractéristiques de technologie RFID

Lorsque la technologie RFID est associée à l'informatique, elle forme ce que l'on appelle un système RFID. Ce système est principalement constitué des éléments suivants :

- Un ou plusieurs tags
- Une antenne
- Un lecteur ou interrogateur
- Une infrastructure de communication

- Un logiciel d'application, comprenant une base de données utilisateur, une application et une interface.

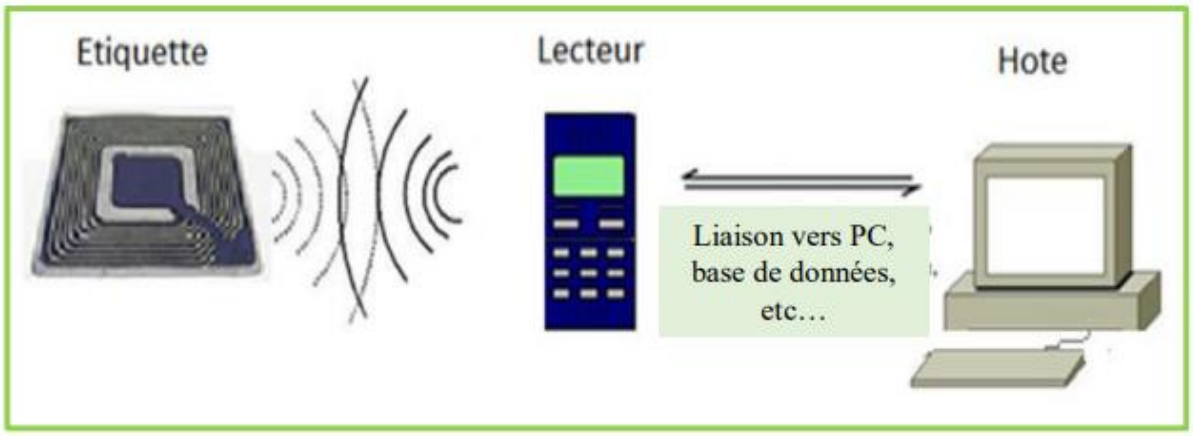


Figure 1. 22 : Composants d'un système RFID.

1.5.3.3Principe de fonctionnement de technologie RFID

La technologie RFID est basée sur l'émission de champ électromagnétique par le lecteur qui est reçu par l'antenne d'une ou de plusieurs étiquettes. Le lecteur émet un signal selon une fréquence déterminée vers une ou plusieurs étiquettes situées dans son champ de lecture.

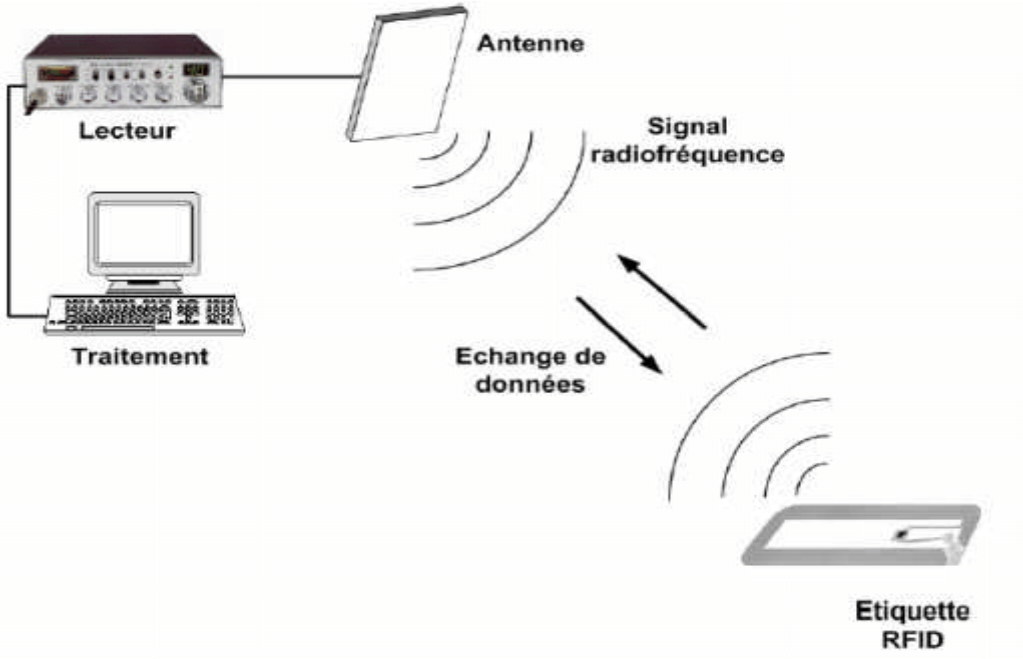


Figure 1. 23 : Principe de fonctionnement RFID [25].

- **Tag RFID**

Il s'agit d'un petit dispositif électronique composé d'une puce et d'une antenne. La puce contient des informations spécifiques, telles qu'un identifiant unique ou des données spécifiques à l'objet auquel elle est attachée. L'antenne est utilisée pour communiquer avec le lecteur RFID via des ondes radio.

Figure 1. 24 : Tag RFID.

- **Antenne**

Elle est utilisée pour émettre et recevoir des signaux radiofréquences entre le lecteur et les tags RFID. L'antenne du lecteur émet le signal pour activer les tags et recevoir les données qu'ils contiennent.

- **Infrastructure de communication**

Cette infrastructure comprend les équipements nécessaires pour transmettre les données collectées par les lecteurs RFID vers les systèmes informatiques de l'entreprise. Cela peut inclure des réseaux filaires ou sans fil, des passerelles de communication, des routeurs, etc.

- **Logiciel d'application**

C'est le logiciel qui gère les données collectées par les lecteurs RFID. Il peut s'agir d'une base de données pour stocker les informations sur les tags RFID, d'une application pour traiter et analyser ces données, et d'une interface utilisateur pour interagir avec le système RFID. Ce logiciel peut être personnalisé en fonction des besoins spécifiques de l'entreprise, notamment en ce qui concerne la gestion des stocks, la traçabilité des produits, la gestion des actifs, etc.

- **Lecteur RFID**

Le dispositif RFID, souvent désigné sous le nom de lecteur/enregistreur RFID, se compose d'un circuit émettant une énergie électromagnétique par le biais d'une antenne, ainsi que d'une unité électronique recevant et interprétant les données transmises par le transpondeur. Ces données sont ensuite relayées au dispositif de collecte des données. Le lecteur RFID est chargé de lire les étiquettes radiofréquence et de transmettre les informations qu'elles contiennent vers la couche suivante du système, appelée middleware [26].

Un lecteur RFID permet :

- La gestion de la communication avec le tag (activation, ouverture de session, lecture, écriture, autorisation...) ;
- La gestion du transport des données (fréquence, vitesse de transfert, modulation, puissance d'émission...) ;
- Le codage, le décodage, le contrôle et le stockage des données ;

Figure 1. 25 : Lecteur RFID.

- **Middleware RFID**

Les anciens systèmes fonctionnaient de manière centralisée, signifiant que toutes les données étaient récupérées par une seule application. Cependant, avec l'évolution des besoins des entreprises, il est devenu impératif de partager ces données avec les partenaires, notamment les fournisseurs. Pour répondre à cette demande croissante, l'architecture des systèmes RFID a été révisée pour intégrer un nouveau composant logiciel : un middleware ou intergiciel RFID. Ce middleware tire parti de l'architecture distribuée de la technologie RFID, facilitant la collaboration entre différentes applications. La Figure 26 illustre la composition en couches de cette nouvelle architecture [27].

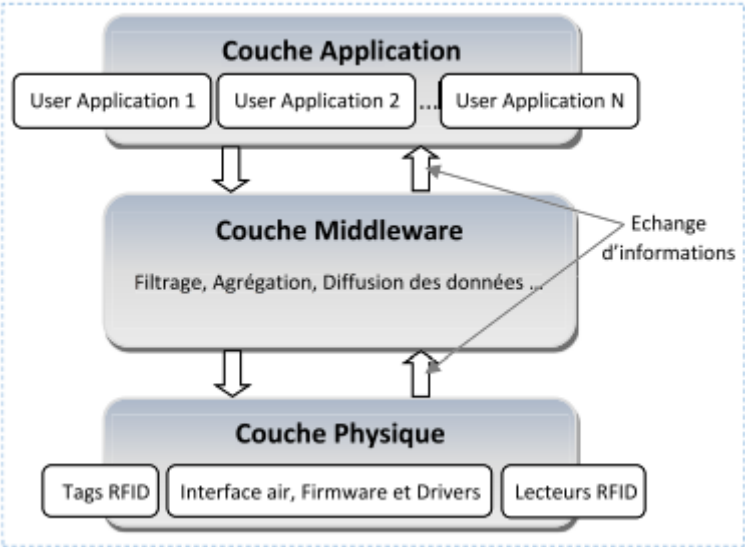


Figure 1. 26 : Architecture en couches d'un système RFID.

1.6 Conclusion

Dans ce chapitre, nous avons présenté différents systèmes de pointages comme les systèmes biométriques, ainsi que la technologie principale empreinte digitale et RFID, les architectures et les fonctionnalités de ces technologies ont été discutées en profondeur.

Pour le prochain chapitre, nous allons présenter notre système sous forme d'une description pour bien comprendre le déroulement.

Chapitre 2
Description du système de pointage et de contrôle d’accès

2.1 Introduction

Chaque jour, il est observé une augmentation significative du nombre de personnes accédant aux locaux bancaires, que ce soit dans des contextes professionnels tels que les entreprises ou dans des contextes résidentiels tels que les domiciles. Cette expansion a mis en évidence plusieurs déficits en matière de surveillance et de gestion des accès des employés. Afin de pallier ces lacunes et d'optimiser la gestion des flux au sein de ces établissements, nous préconisons la mise en place d'un système de pointage automatisé. Ce dernier repose sur une combinaison de l'identification par empreinte digitale et l'utilisation de cartes RFID. Dans ce chapitre, nous exposerons en détail le schéma synoptique ainsi que les différents outils nécessaires à la conception et à l'implémentation de ce dispositif [27].

2.2 Architecture générale du système

Dans le cadre de ce projet, nous présentons un organigramme pour la description d'un système de pointage et de contrôle d'accès innovant basé sur la technologie d'empreinte digitale et de RFID pour une banque. Ce système vise à moderniser et à rationaliser le processus de gestion des présences des employés tout en renforçant la sécurité des installations bancaires. L'organigramme fournit une vue d'ensemble structurée des différentes étapes :

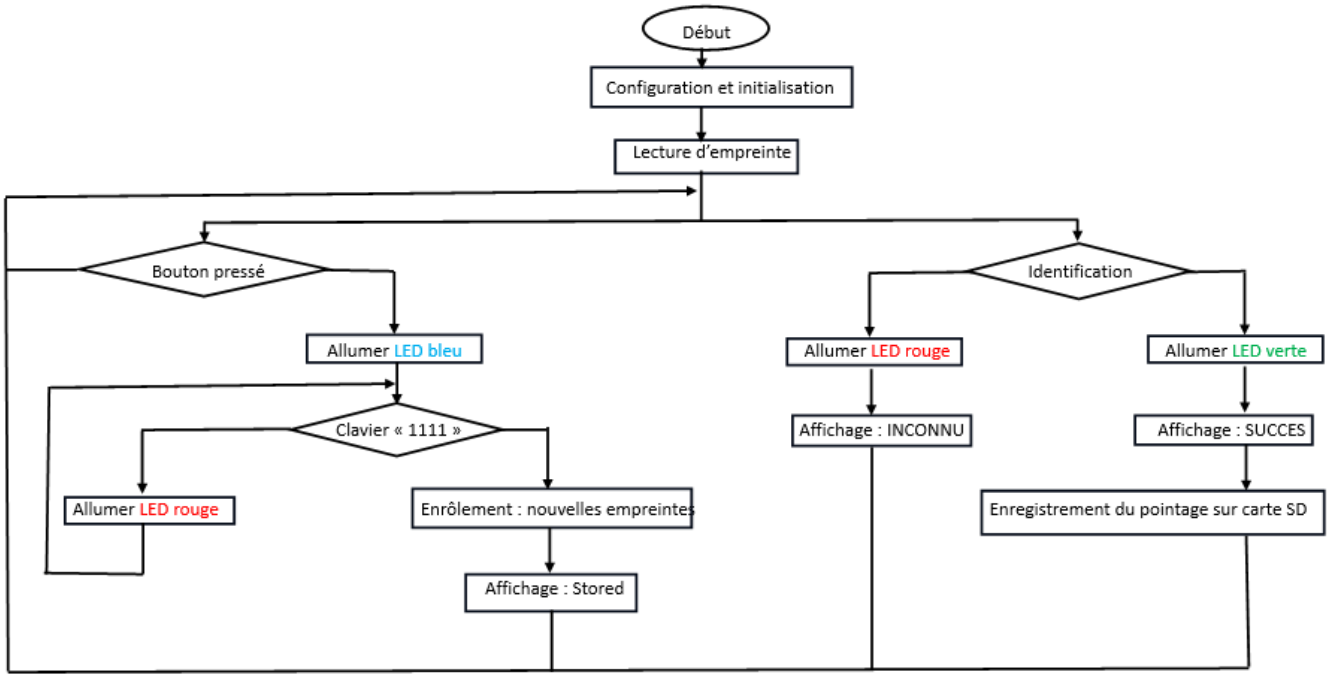


Figure 2. 1 : Schéma synoptique de système de pointage

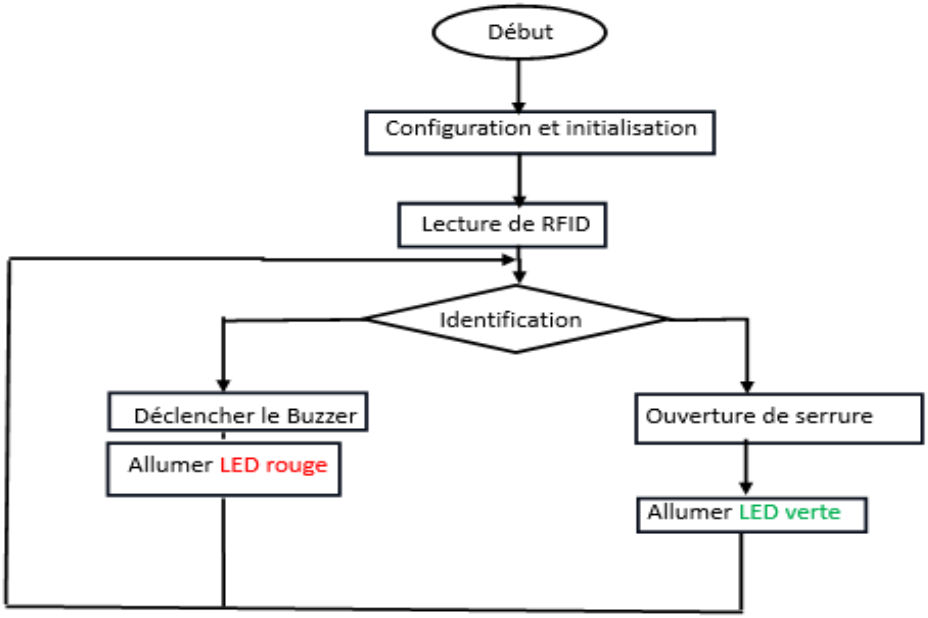


Figure 2. 2 : Schéma synoptique de système de contrôle d'accès.

2.3 Architecture matérielle du système

Comprendre l'architecture matérielle d'un système est essentiel pour saisir son fonctionnement et ses performances. Elle vise à présenter les principaux composants matériels du système et leur rôle dans son fonctionnement global. Une connaissance de l'architecture matérielle permet de mieux appréhender les capacités, les limitations et les possibilités d'optimisation du système.

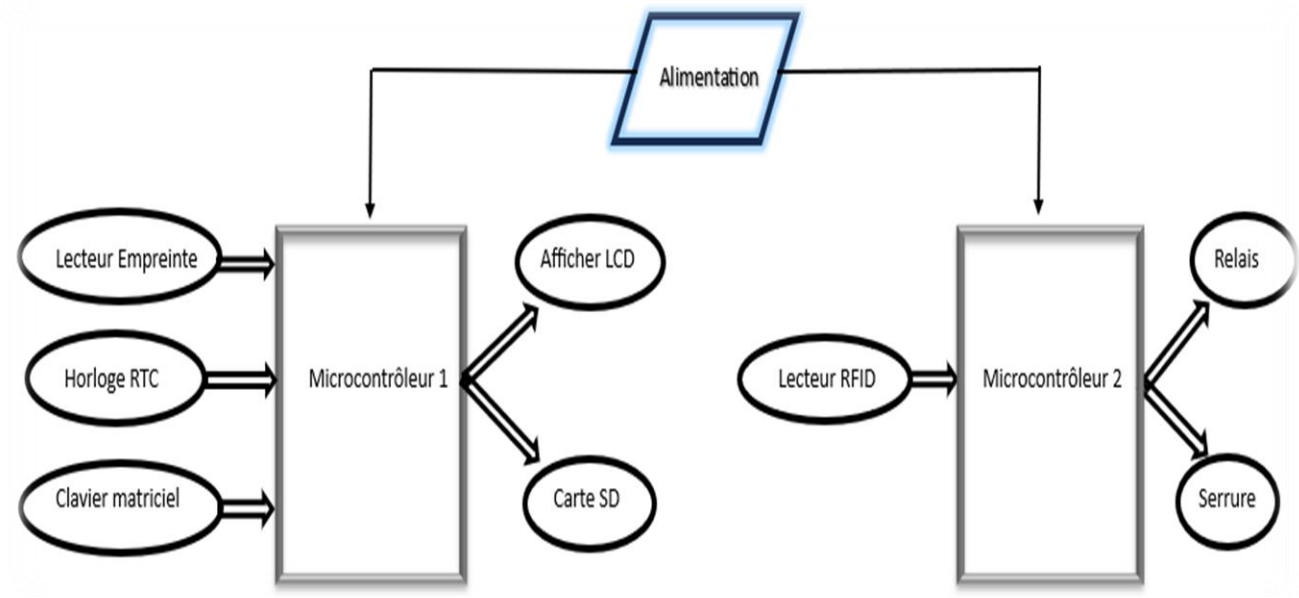


Figure 2. 3 : Architecture matérielle du système.

2.4 Description des capteurs d'empreinte digitale

Les capteurs d'empreinte digitale jouent un rôle crucial dans l'identification et l'authentification des individus. Ils permettent de comparer la signature de l'empreinte digitale d'un utilisateur avec celles stockées dans une base de données, que ce soit pour une utilisation mono ou pluri utilisateurs. Chaque empreinte digitale est unique, constituant ainsi une carte d'identité biologique précise pour chaque personne. La science qui étudie les empreintes digitales est appelée la dactyloscopie.

Différents types de capteurs d'empreintes digitales existent, chacun utilisant une technologie spécifique pour capturer et analyser les empreintes digitales. Voici une liste des principaux types de capteurs d'empreintes digitales :

2.4.1 Capteurs optiques

De nombreuses entreprises, telles que Identix et Sagem, commercialisent actuellement plusieurs systèmes de capture d'empreintes digitales basés sur des capteurs optiques, notamment des capteurs matriciels de type CCD ou APS. Ces systèmes exploitent principalement le principe de réflexion de la lumière pour détecter et enregistrer les caractéristiques des empreintes digitales. Les capteurs optiques utilisés dans ces systèmes sont réputés pour leur simplicité, leur coût abordable et leur capacité à produire des images de haute résolution. Cependant, ils sont également confrontés à des défis, notamment leur sensibilité aux variations de luminosité et la possibilité de laisser des empreintes digitales latentes, ce qui nécessite un entretien régulier pour maintenir des performances optimales. Malgré ces limitations, les capteurs optiques demeurent populaires dans de nombreuses applications biométriques en raison de leur fiabilité et de leur coût relativement bas[28].

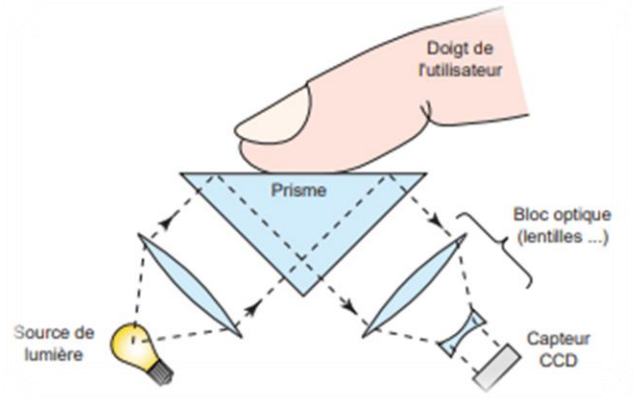


Figure 2. 4 : Principe de fonctionnement d'un capteur d'empreintes digitales optique [29].

2.4.2 Capteurs capacitifs

Le principe de fonctionnement d'un capteur d'empreinte digitale capacitif utilisant des électrodes obtenues par croissance électrolytique consiste à polariser la surface du doigt pour détecter et enregistrer les empreintes digitales. Ce type de capteur comporte une grille de pixels, où chaque pixel est constitué

d'une électrode obtenue par croissance électrolytique, généralement en cuivre ou en métal noble, et d'un matériau diélectrique.

Lorsque le doigt de l'utilisateur entre en contact avec le capteur, les électrodes polarisées induisent une variation de capacitance, qui est détectée par le capteur. Cette variation est mesurée à chaque pixel de la matrice, permettant ainsi de créer une image détaillée de l'empreinte digitale.

Le substrat du capteur est généralement en silicium, offrant une base solide pour les électrodes et les composants électroniques intégrés. Les transistors sont utilisés pour amplifier et traiter les signaux capacitifs générés par le contact du doigt avec le capteur. Ils sont généralement fabriqués à partir de semi-conducteurs tels que le silicium.

Après la capture de l'image de l'empreinte digitale, celle-ci est analysée et comparée aux empreintes digitales enregistrées pour l'identification ou l'authentification de l'utilisateur.

Les capteurs d'empreinte digitale capacitifs utilisant des électrodes obtenues par croissance électrolytique offrent une sensibilité élevée, une grande précision et une résistance accrue aux conditions environnementales. Cependant, leur fabrication peut être plus complexe en raison de la nécessité de produire des électrodes par croissance électrolytique [29].

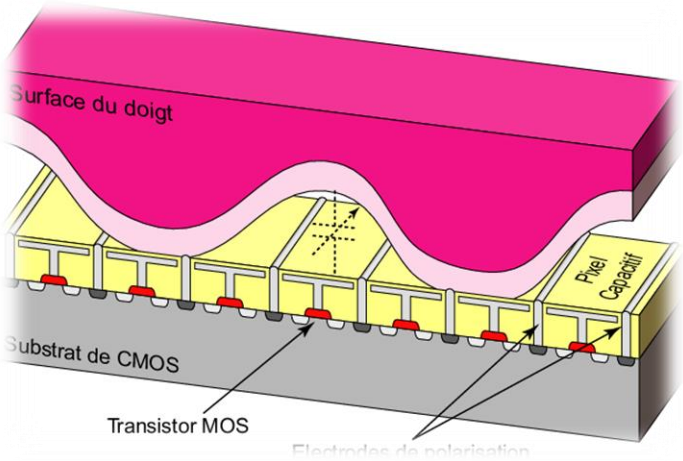


Figure 2. 5 : Capteur capacitif utilisant des électrodes obtenues par croissance électrolytique afin de polariser la surface du doigt.

2.4.3 Capteurs à ultrasons

Le fonctionnement d'un capteur d'empreinte digitale ultrasonique repose sur l'utilisation d'un émetteur/récepteur d'ultrasons en rotation. Ce dispositif émet des ondes sonores à haute fréquence vers la surface de l'empreinte digitale. Ces ondes, généralement des ultrasons, rebondissent sur la surface de la peau, enregistrant ainsi des informations sur les crêtes et les vallées de l'empreinte. En capturant les ondes réfléchies, le capteur peut calculer la distance entre lui-même et chaque point de l'empreinte, permettant ainsi de reconstruire une image tridimensionnelle détaillée. Cette image est ensuite analysée pour l'authentification ou l'identification de l'utilisateur. Les capteurs ultrasoniques offrent une sécurité accrue

en détectant les caractéristiques sous la surface de la peau, ainsi qu'une meilleure résistance aux conditions environnementales. Cependant, leur production peut être plus coûteuse et nécessiter des composants plus complexes que d'autres types de capteurs, comme les capteurs optiques ou capacitifs[30].

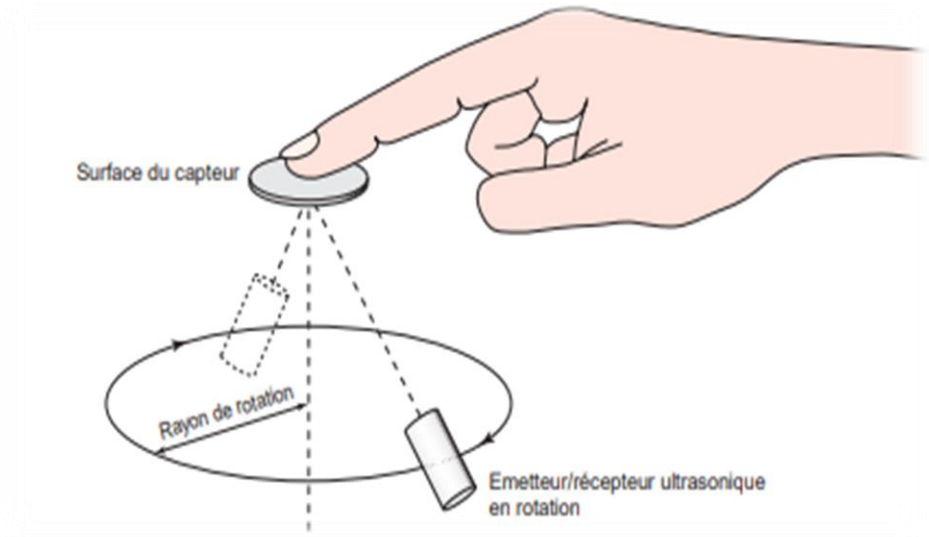


Figure 2. 6 : Principe de fonctionnement d'un capteur d'empreintes digitales ultrasonique à émetteur/récepteur en rotation [30].

2.4.4 Capteurs thermiques

La méthode thermique, bien que moins courante, est illustrée par le FingerChip fabriqué par Atmel. Ce capteur thermique est le seul de son genre actuellement disponible. Il offre une qualité d'image excellente même avec des empreintes de qualité médiocre, ce qui en fait l'un des capteurs les plus résistants par rapport aux autres technologies. Les capteurs thermiques mesurent les variations de température à la surface de l'empreinte digitale en détectant les différences de conductivité thermique entre les crêtes et les vallées. Bien que moins répandus que les autres types de capteurs, ils présentent des avantages en termes de robustesse et de performance dans des environnements difficiles [31].

Figure 2. 7 : les crêtes et les vallées d'empreinte [31].

2.5 Description des lecteurs RFID

Les lecteurs RFID sont des dispositifs utilisés pour lire les informations stockées sur des étiquettes RFID, émettant des signaux radiofréquence pour interroger les étiquettes à proximité. Ils sont disponibles sous différentes formes, notamment fixes, portables et embarqués, et sont équipés de composants tels que des antennes, des modules de lecture/écriture, des unités de traitement et des interfaces de communication. Ces lecteurs sont largement utilisés dans des domaines tels que la logistique, la gestion des stocks, le contrôle d'accès et la sécurité.

Il existe plusieurs types de capteurs RFID, chacun étant conçu pour répondre à des besoins spécifiques en termes de portée, de fréquence de fonctionnement et d'applications [32].

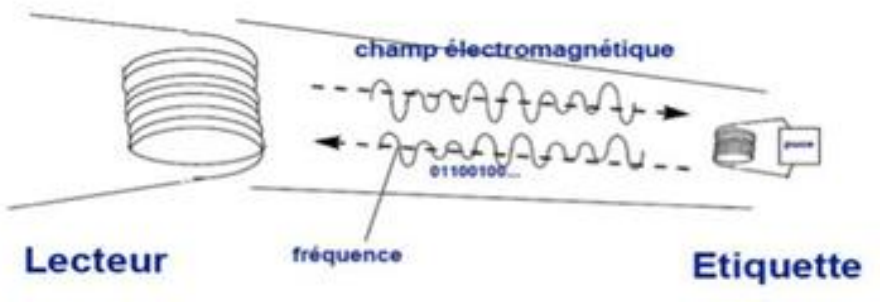


Figure 2. 8 : RFID basé sur la fréquence.

Voici une description des principaux types de capteurs RFID :

2.5.1 Capteurs RFID passifs

Les capteurs RFID passifs ne disposent pas d'une alimentation interne. Ils sont activés par les signaux radiofréquence émis par un lecteur RFID et renvoient les données stockées dans leur mémoire en réponse. Ces capteurs sont principalement employés dans des domaines tels que la gestion des stocks, le suivi des actifs et les systèmes de badges d'accès[33].

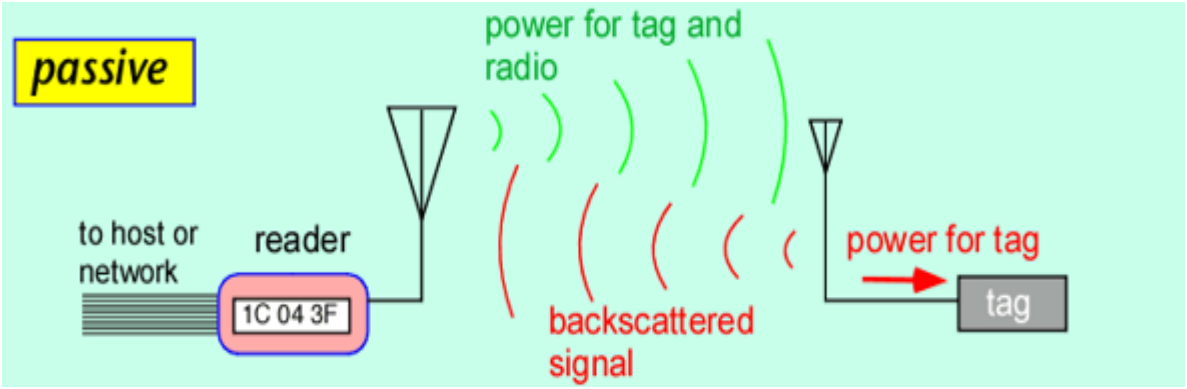


Figure 2. 9 : RFID passive [33].

2.5.2 Capteurs RFID semi-passifs

Les capteurs RFID semi-passifs sont dotés d'une source d'alimentation interne réduite, mais restent tributaires des signaux radiofréquence du lecteur pour la communication. Ils offrent une portée améliorée par rapport aux capteurs passifs, tout en conservant une consommation d'énergie minimale. Ces capteurs sont fréquemment employés dans des contextes comme le suivi d'objets mobiles et la surveillance de l'environnement [33].

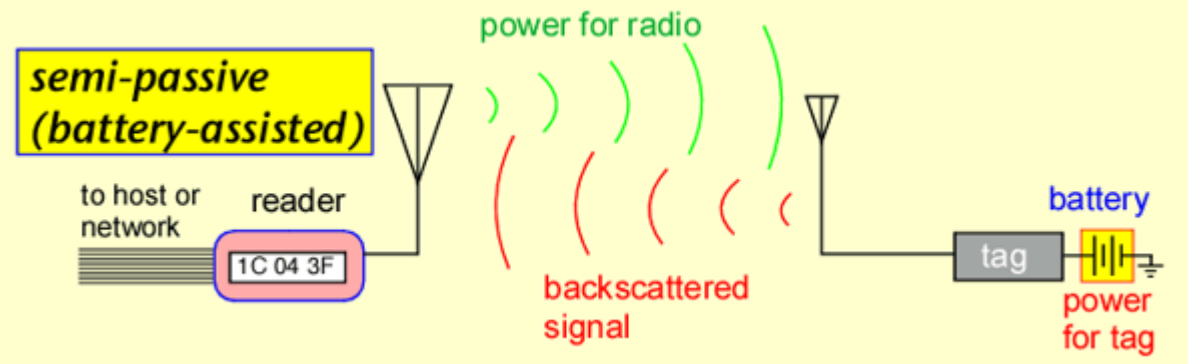


Figure 2. 10 : RFID semi-passive [33].

2.5.3 Capteurs RFID actifs

À la différence des capteurs passifs, les capteurs RFID actifs intègrent une source d'alimentation, leur permettant d'émettre activement des signaux radiofréquence. Ils sont déployés dans des contextes nécessitant une couverture plus étendue et une communication bidirectionnelle, tels que le suivi de flottes de véhicules, la surveillance des températures et la gestion logistique en temps réel [33].

Figure 2. 11 : RFID active[33].

Qu'est-ce qu'une fréquence ?

La fréquence fait référence au nombre d'ondes traversant un objet fixe dans un temps donné. Par exemple, si une onde met 0.5 seconde pour traverser un objet, la fréquence sera de deux ondes par seconde. Plus la fréquence est élevée, plus le nombre d'ondes qui traversent cet objet particulier par temps donné (généralement par seconde) est élevé [34].

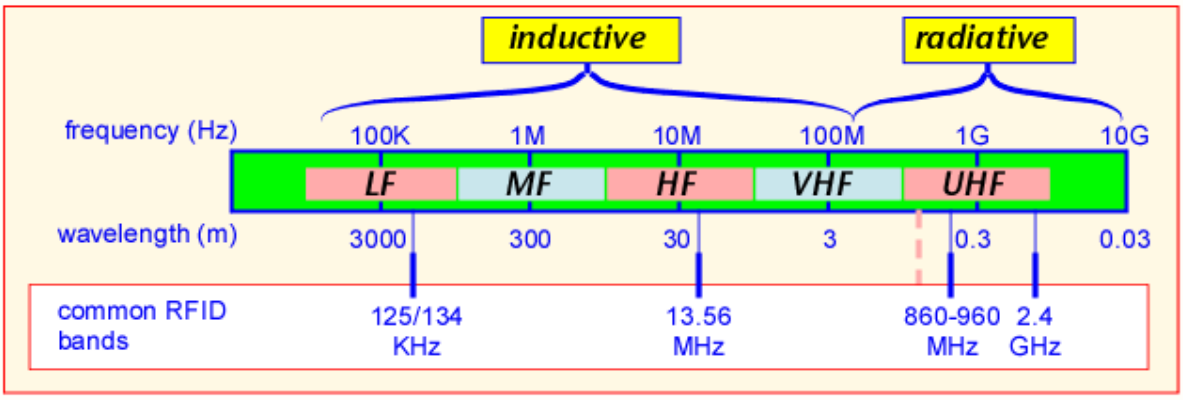


Figure 2. 12 : Bandes de fréquences courantes utilisées pour la RFID [34].

2.5.4 Capteurs RFID LF

Les capteurs RFID LF (Low Frequency) détectent et lisent les étiquettes RFID fonctionnant à basse fréquence, généralement entre 120 kHz et 140 kHz. Ils émettent un champ magnétique pour activer les étiquettes à proximité, ce qui permet la transmission des données stockées dans ces étiquettes. Ces capteurs sont largement utilisés dans des applications telles que le contrôle d'accès, la gestion des animaux, le suivi des actifs et la logistique, offrant une lecture fiable et précise avec une faible sensibilité aux interférences électromagnétiques[35].

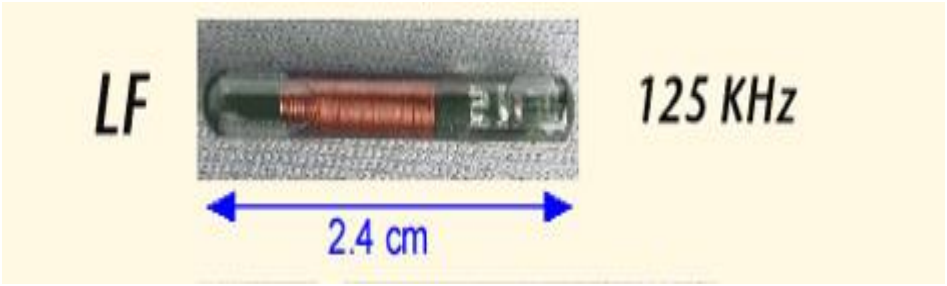


Figure 2. 13 : RFID LF [35].

2.5.5 Capteurs RFID HF

Les capteurs RFID HF fonctionnent dans la plage de fréquences élevées, généralement autour de 13,56 MHz. Ils offrent une portée de lecture plus courte que les capteurs UHF, mais une meilleure précision et une communication plus rapide. Ces capteurs sont souvent utilisés dans les applications de contrôle d'accès, de paiement sans contact et de gestion des bibliothèques.

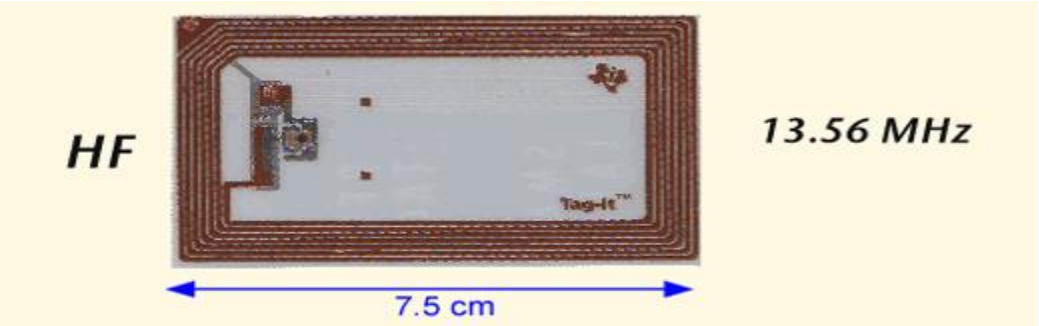


Figure 2. 14 : RFID HF [36].

2.5.6 Capteurs RFID UHF

Les capteurs RFID UHF fonctionnent dans la plage de fréquences ultra-hautes, généralement entre 868 et 915 MHz. Ils offrent une portée de lecture plus étendue et une capacité à lire plusieurs étiquettes simultanément. Ces capteurs sont largement utilisés dans les applications de suivi des produits, de la chaîne d'approvisionnement et de la logistique [37].

Figure 2. 15 : RFID UHF [37].

2.6 Composants matériels et logiciels

2.6.1 Outils matériels

Ils sont utilisés pour construire le système, ainsi que pour tester et déboguer leur fonctionnement.

2.6.1.1 Microcontrôleurs

La carte Arduino est une plateforme d'objets interactifs à usage créatif utilisée pour réaliser des projets électroniques plus développé. Elle est composée d'un circuit physique programmable dit microcontrôleur, et d'un logiciel qui est utilisé pour créer et télécharger un code de l'ordinateur à la carte [38].

Microcontrôleur 1 : **Arduino MEGA 2560**

L'Arduino Méga 2560 est le microcontrôleur basé sur un ATmega2560 le plus puissant de la gamme en termes de performances, de capacité de mémoire et de possibilité de connecter un très grand nombre de périphériques à la carte.

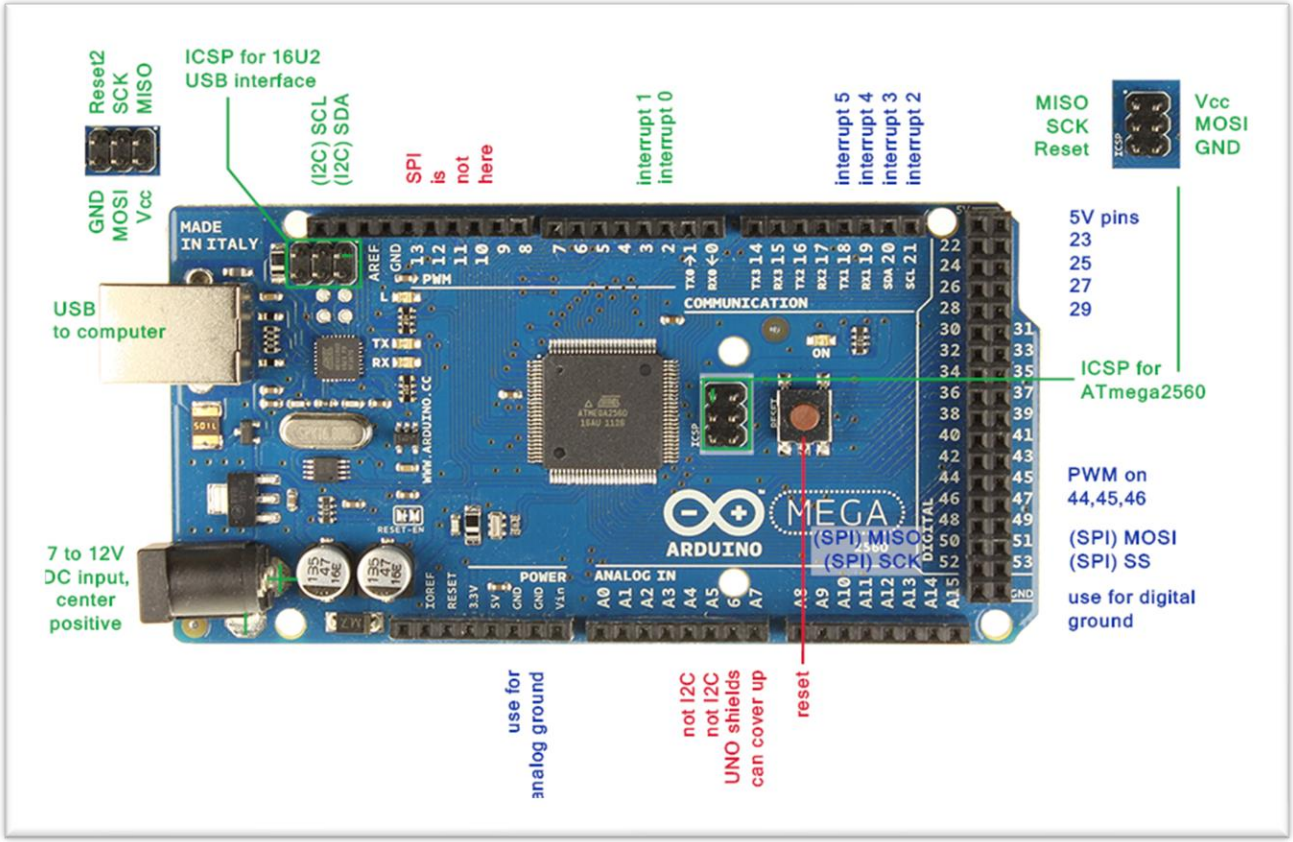


Figure 2. 16 : Carte Arduino Méga.

Microcontrôleur 2 : **Carte Arduino NANO**

Il s'agit d'une petite carte basée sur les microcontrôleurs comme l'ATmega328P sinon l'ATmega628 mais la connexion de cette carte est la même que celle de la carte Arduino UNO. Ce type de carte microcontrôleur est de très petite taille, durable, flexible et fiable [29].

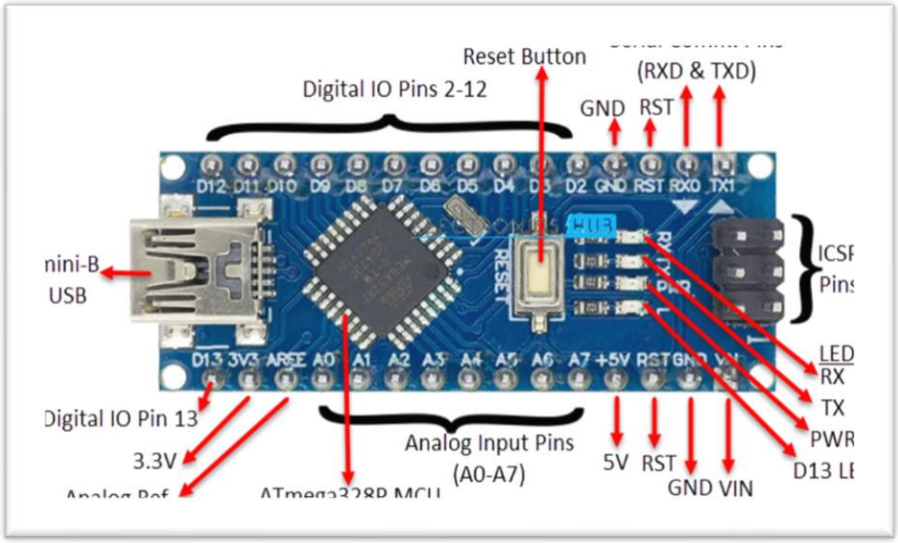


Figure 2. 17 : Carte Arduino Nano.

2.6.1.2 Alimentation

L'Arduino Méga peut être alimenté soit avec une tension de 7 à 12 volts via la prise d'alimentation, soit avec une tension de 5 volts via le connecteur USB. Il intègre un régulateur de tension qui réduit la tension d'entrée à 5 volts pour alimenter ses composants internes.

De même, l'Arduino Nano peut être alimenté avec une tension de 7 à 12 volts via la broche VIN ou avec une tension de 5 volts via le connecteur USB. Comme l'Arduino Méga, il est équipé d'un régulateur de tension intégré pour adapter la tension d'entrée à celle nécessaire pour ses composants internes.

2.6.1.3 Mémoire de stockage

La mémoire EEPROM est un type de mémoire non volatile conçue pour stocker des données de manière permanente dans un microcontrôleur ou un dispositif électronique. Contrairement à la mémoire RAM qui perd son contenu en cas de coupure d'alimentation, la mémoire EEPROM conserve les données même lorsque l'alimentation est coupée. Ces mémoires sont largement utilisées dans divers systèmes embarqués tels que les microcontrôleurs Arduino, les cartes Raspberry Pi, ESP et autres, ainsi que dans les appareils électroniques grand public et les systèmes de stockage de données. Elles offrent une solution pratique pour stocker des configurations, des paramètres utilisateur et des données de calibration de manière permanente.

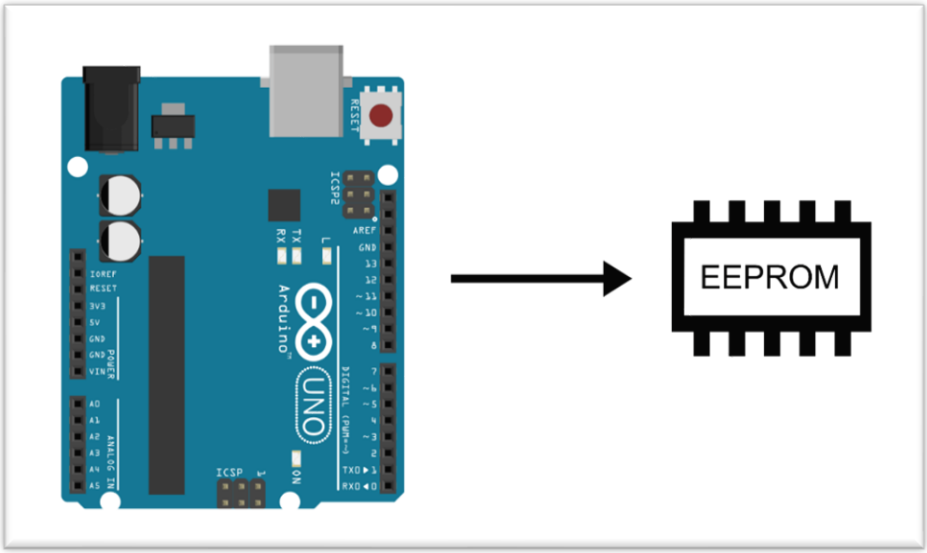


Figure 2. 18 : Mémoire de stockage EEPROM Arduino [39].

2.6.1.4 Entrées

- **Lecteur Empreinte Digitale**

Le capteur d'empreinte digitale optique utilise une technologie optique avancée pour capturer les empreintes digitales en illuminant le doigt avec une lumière verte. Ensuite, un processeur numérique traite l'image capturée pour extraire les caractéristiques spécifiques de l'empreinte. Ces caractéristiques sont converties en un identifiant unique à l'aide d'algorithmes sophistiqués, qui est comparé aux empreintes digitales enregistrées pour vérifier l'identité de l'utilisateur.

Il existe dans l'empreinte digitale 6 broches : deux pour la communication avec ARDUINO (Tx, Rx) et deux pour l'alimentation (VCC et GND), les deux autres broches pour d'autre fonctionnalité non utiliser dans notre système.

Figure 2. 19 : Les broches d'un capteur d'empreinte digitale.

- **Horloge RTC**

Les modules RTC, ou horloges en temps réel, sont des dispositifs conçus pour mémoriser l'heure et la date. Ils intègrent une batterie qui leur permet de fonctionner même en l'absence d'alimentation externe, garantissant ainsi la conservation de l'heure et de la date. Ainsi, les modules RTC fournissent une référence précise de l'heure et de la date, même lorsque le projet est hors tension ou lors de la reprogrammation d'un microcontrôleur, grâce à leur alimentation par pile [40].

Figure 2. 20 : Module RTC-DS3231.

- **Clavier matriciel**

Le clavier est l'unité de saisie du code secret pour coder, de clavier à utiliser est un clavier 7 broches 4x3 (4 lignes et 3 colonnes), les quartes premières broches sont destinées aux lignes, et les trois dernières destinées pour les colonnes [41].

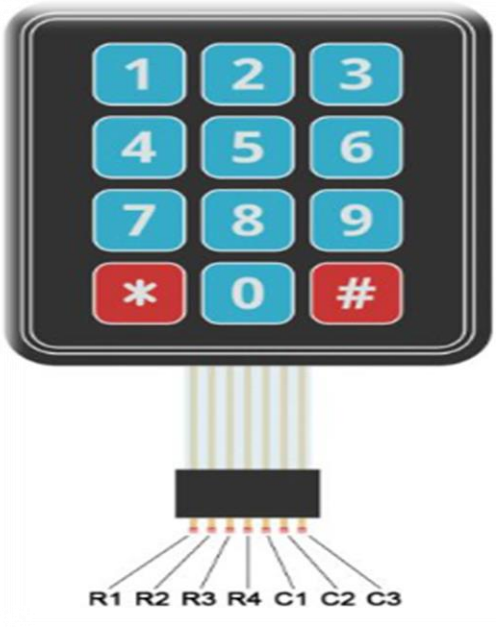


Figure 2. 21 : clavier matriciel (4x3).

➢ **Lecteur RFID**

Il s'agit d'un dispositif passif émetteur-récepteur radio bidirectionnel utilisé pour communiquer avec les étiquettes RFID. Fonctionnant à une fréquence de 13,56 MHz (basse fréquence), il crée un champ électromagnétique permettant d'interagir avec les tags. Basé sur le circuit intégré MFRC522, ce lecteur communique avec un microcontrôleur via une interface périphérique série (SPI) offrant un débit de données maximal de 10 Mbps. De plus, il prend en charge la communication via les protocoles I2C et UART [42].

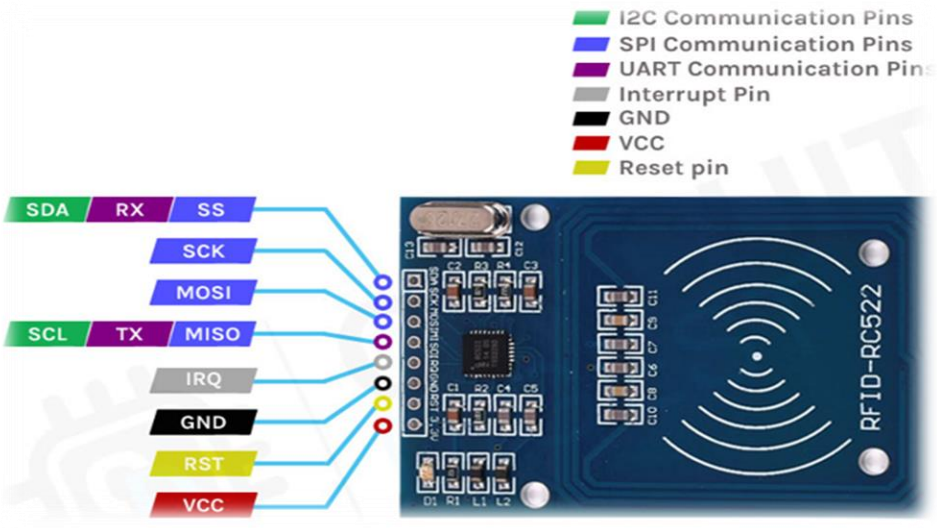


Figure 2. 22 : Broches module RFID-RC522.

2.6.1.5 Sorties

➢ **Afficheur LCD**

L'écran LCD joue un rôle crucial dans la visualisation des informations échangées entre l'utilisateur et le microcontrôleur. Il permet d'afficher divers messages administratifs, tels que l'enregistrement ou la lecture d'empreintes, ainsi que l'état des capteurs et le journal des événements. Nous avons opté pour un écran LCD 16x2, offrant 2 lignes et 16 colonnes, et nous utilisons un module I2C pour minimiser la charge sur la carte Arduino en réduisant le nombre de broches utilisées[43].

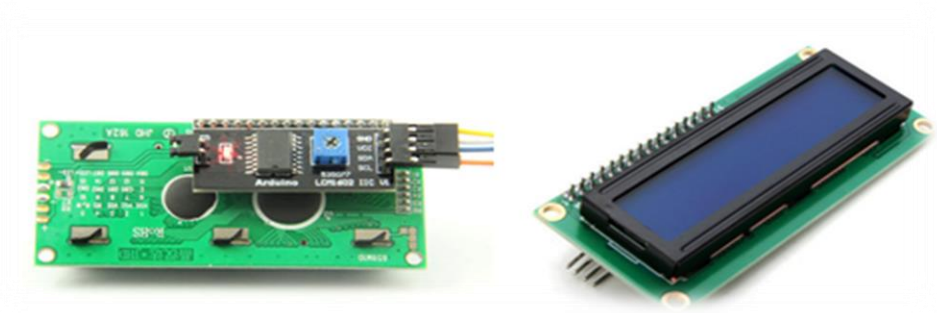


Figure 2. 23 : Afficheur LCD avec module I2C.

- **Lecteur carte SD**

Le lecteur de carte SD Arduino est un périphérique électronique permettant à un microcontrôleur Arduino d'interagir avec une carte mémoire SD. Il utilise généralement une interface de communication simple comme le bus SPI pour transférer des données entre la carte Arduino et la carte SD, facilitant ainsi la lecture et l'écriture de fichiers et de données [44].

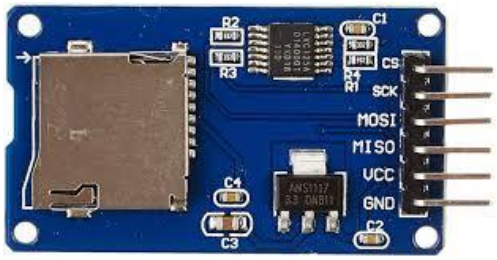


Figure 2. 24 : Lecteur carte SD.

- **Serrure électromagnétique**

Une serrure électromagnétique est un mécanisme de verrouillage qui utilise le magnétisme pour sécuriser une porte. Elle est constituée d'une plaque de fixation et d'un électroaimant. Lorsque l'électroaimant est activé par une impulsion électrique, il crée un champ magnétique qui attire la plaque de fixation, verrouillant ainsi la porte de manière sécurisée. Ces serrures sont couramment utilisées dans les systèmes de contrôle d'accès pour offrir un niveau élevé de sécurité et de contrôle, elles sont alimentées par 12V [45].

Figure 2. 25 : Serrure électromagnétique.

- **Module relais**

Le module de relais 5V est un dispositif utilisé pour contrôler des circuits électriques en fonction d'un signal numérique provenant d'un microcontrôleur ou d'une puce logique. Il fonctionne avec une tension de déclenchement de bas niveau de 5V DC et peut être utilisé pour activer ou désactiver un circuit électromagnétique. Ce module se compose principalement d'un relais électromagnétique et d'un module de commande.

Figure 2. 26 : module relais.

- Le relais contient la bobine qui crée le champ magnétique, l'armature qui se déplace pour terminer ou déconnecter un circuit, et les contacts qui s'ouvrent et se ferment pour actionner l'interrupteur de charge.
- Le module de contrôle de relais est l'interface ou la partie du module de relais avec laquelle l'utilisateur interagit. Il contient les bornes d'entrée pour la connexion au microcontrôleur, ainsi que les bornes de sortie pour la connexion à la charge.
- Le module de commande contient également Indicateurs LED pour l'alimentation et l'état et d'autres dispositifs tels que la diode de protection, le transistor, la résistance et d'autres dispositifs à semi-conducteurs nécessaire à son fonctionnement.

2.6.2 Outils logiciels

Ils englobent les programmes informatiques utilisés pour concevoir, développer, tester et exploiter des systèmes informatiques et électroniques. Ils comprennent divers éléments tels que les environnements de développement intégrés (IDE), les langages de programmation, les bibliothèques de logiciels, les systèmes d'exploitation, les outils de simulation, les outils de modélisation, les logiciels de conception assistée par ordinateur (CAO), entre autres. Ces outils logiciels sont indispensables pour la programmation et la gestion des systèmes, ainsi que pour l'analyse et la manipulation des données.

2.4.2.1 Logiciel de programmation Arduino IDE

L'IDE Arduino, un environnement de développement intégré, utilise un langage de programmation dérivé du langage Wiring, lui-même une version simplifiée de C/C++. Ce langage vise à rendre la programmation sur les microcontrôleurs Arduino accessible à un large public, en simplifiant certaines complexités du C/C++ tout en conservant une souplesse suffisante pour des projets avancés.

Cette simplification syntaxique offre plusieurs avantages : une syntaxe plus claire et plus facile à comprendre, une abstraction matérielle qui simplifie l'interaction avec les composants électroniques, des bibliothèques intégrées qui facilitent la programmation de tâches courantes, et une interface conviviale dans l'IDE Arduino qui rend le processus de développement plus intuitif.

En somme, le langage de programmation utilisé dans l'IDE Arduino combine les aspects les plus utiles du C/C++ avec une approche simplifiée et accessible, en faisant ainsi un choix idéal pour les débutants et les amateurs qui souhaitent se lancer dans la programmation sur microcontrôleurs [46]

2.4.2.2 Différents systèmes basés sur langage Arduino :

L'IDE Arduino est employée dans une diversité de secteurs, couvrant une large gamme d'applications

- **Physical Computing :** Ce domaine implique la création de systèmes physiques interactifs qui utilisent des logiciels et du matériel pour interagir avec des capteurs et des actionneurs.
- **Électronique industrielle et embarquée :** Arduino est utilisé pour développer des systèmes de contrôle industriels, des automates programmables et des solutions embarquées.
- **Art / Spectacle :** De nombreux artistes s'en servent pour créer des œuvres interactives, des installations lumineuses et des performances artistiques.
- **Domotique :** Arduino est employé dans l'automatisation et le contrôle des systèmes domestiques comme l'éclairage, la sécurité et le chauffage.
- **Robotique :** Il est utilisé dans la conception et le contrôle de robots pour diverses applications, de l'éducation à la recherche.
- **Modélisme :** Les amateurs de modélisme l'utilisent pour contrôler et automatiser des maquettes de trains, d'avions et d'autres modèles réduits.
- **DIY (Do-It-Yourself), Hacker, Prototypage, Éducation, etc. :** Arduino est couramment employé dans les projets DIY, les communautés de hackers, le prototypage rapide et l'éducation pour enseigner les principes de l'électronique et de la programmation.
- En somme, l'IDE Arduino est un outil polyvalent et accessible qui trouve des applications dans une multitude de domaines, de l'art à l'industrie, en passant par le divertissement et l'éducation[47].

2.4.2.3 Bibliothèques utilisées

Sur Arduino, il existe de nombreuses bibliothèques logicielles qui facilitent le développement de projets en fournissant des fonctions et des routines prêtes à l'emploi [48].

Voici les bibliothèques utilisées sur Arduino :

```
#include <Wire.h>
#include <Adafruit_Fingerprint.h>
#include <RTClib.h>
#include <LiquidCrystal_I2C.h>
#include <SD.h>
#include <Keypad.h>

#include <SPI.h>
#include <MFRC522.h>
```

Figure 2. 27 : Bibliothèques Arduino utilisées pour le système.

- **Wire.h :** Utilisée pour communiquer avec des dispositifs I2C (Inter-Integrated Circuit).
- **Adafruit_Fingerprint.h :** utilisée avec les modules de capteurs d'empreintes digitales d'Adafruit. Elle permet de communiquer avec ces capteurs pour capturer, stocker et vérifier les empreintes digitales.
- **RTClib.h :** utilisée pour faciliter la gestion de l'horloge en temps réel (RTC) dans les projets électroniques.
- **LiquidCrystal_I2C.h :** utilisée pour faciliter l'utilisation d'écrans LCD basés sur le protocole de communication I2C (Inter-Integrated Circuit). Cette bibliothèque est une extension de la bibliothèque LiquidCrystal standard d'Arduino, conçue spécifiquement pour les écrans LCD utilisant une interface I2C.
- **SD.h :** Utilisée pour lire et écrire sur une carte mémoire SD.
- **Keypad.h :** utilisée pour saisir des données dans de nombreux projets. Simplifie l'utilisation des claviers matriciels dans les projets.
- **SPI.h :** Utilisée pour communiquer avec des dispositifs SPI .
- **MFRC522.h :** utilisée pour faciliter l'utilisation des modules RFID (Radio-Frequency Identification) basés sur le circuit intégré MFRC522.

2.7 Description et fonctionnalité du système

Le système de pointage des employés de la banque modernise le processus traditionnel de marquage des présences au stylo et au papier en favorisant l'enregistrement en ligne des présences en un seul geste. Ce module offre aux directeurs la possibilité de gérer et de suivre les informations de présence des

employés depuis leur bureau. En intégrant des dispositifs d'empreinte digitale et de RFID pour le contrôle d'accès, le processus est entièrement automatisé : les employés peuvent scanner leur carte numérique devant le dispositif et leur présence est enregistrée dans le module de gestion des présences par empreinte digitale, facilitant ainsi le suivi des retards et des absences. Ce système rend la gestion quotidienne des présences sans tracas, permettant ainsi de libérer du temps précieux.

Dans le cadre de ce projet, nous concevrons une pointeuse basée sur la technologie d'empreinte digitale et de RFID pour le contrôle d'accès. Chaque employé se voit attribuer une empreinte contenant une identification unique, et leur présence est enregistrée lorsqu'ils placent leur doigt devant le lecteur d'empreinte digitale au début de leur journée de travail. L'accès à la banque en dehors des heures de pointage se fait par carte RFID, ce qui évite la nécessité de multiples pointages tout au long de la journée.

Pour garantir une sécurité maximale, en cas de recrutement de nouveaux employés, le responsable du bureau des acquisitions a la possibilité d'utiliser un bouton d'accès avec un clavier matriciel pour enregistrer de nouvelles empreintes digitales.

2.8 Intégration et avantages du système

Le système de pointage et contrôle d'accès intégrant les technologies d'empreinte digitale et de RFID présente des avantages significatifs en termes de coût et de fonctionnement.

En premier lieu, en optant pour des technologies comme l'empreinte digitale et la RFID, ce système offre un niveau de sécurité élevé tout en restant économique. Les composants requis, tels que les lecteurs d'empreintes digitales et les tags RFID, sont généralement disponibles à des prix concurrentiels sur le marché.

De plus, ce système fonctionne de manière efficace et pratique. L'identification par empreinte digitale offre une méthode fiable et rapide pour le pointage des employés et le contrôle d'accès. De même, la technologie RFID permet une identification sans contact, améliorant ainsi la fluidité du processus et réduisant les délais d'attente.

Par ailleurs, la combinaison de ces deux technologies permet une gestion centralisée des données, simplifiant ainsi la surveillance et le suivi des activités des employés. Les informations de pointage et d'accès sont stockées de manière sécurisée dans une base de données, facilitant la génération de rapports et l'analyse des données.

En somme, le système de pointage et de contrôle d'accès basé sur l'empreinte digitale et la RFID représente un compromis idéal entre sécurité, efficacité et coût, en faisant ainsi une solution attractive pour les entreprises désireuses d'optimiser leur gestion des ressources humaines et leur sécurité globale.

2.9 Conclusion

A travers ce chapitre nous avons présenté l'objectif principal de notre projet, qui est de mettre en œuvre un système de pointage des employés basé sur empreinte digitale et d'accès par RFID. Nous avons ensuite étudié le fonctionnement des différents outils matériels et logiciels que nous allons avoir besoin dans le chapitre suivant, afin de concevoir notre système.

Chapitre 3

Conception du système et essais expérimentaux

3.1 Introduction

Ce chapitre est consacré aux tests et aux résultats de notre projet. Le contenu de ce chapitre est divisé en deux parties : la première consiste présenter le schéma électronique en précisant les branchements de chaque composant avec Arduino méga et nano. La deuxième comporte les tests et les interprétations.

3.2 Méthode d'identification utilisée par notre système

3.2.1 Système de Pointage

La technique d'identification consiste à accorder le pointage après avoir franchi les étapes d'identification et de vérification d'identité, lesquelles sont les suivantes : lecture de l'empreinte via le capteur et confirmation de l'identité en comparant l'empreinte de la personne qui pointe avec celles préalablement identifiées. En cas de confirmation, une LED verte s'allume ; si la personne est inconnue, la LED rouge s'allume. Après le pointage, toutes les empreintes sont enregistrées dans la carte SD sous forme d'un fichier texte indiquant l'identifiant, l'heure et la date. À l'aide d'Excel, il est ensuite possible de connaître les employés par leurs noms et prénoms en utilisant leurs identifiants.

Pour identifier de nouvelles empreintes (employés), il est possible de les ajouter en appuyant sur un bouton, ce qui permet de saisir le mot de passe « 1111 » via le clavier matriciel. Ensuite, l'empreinte souhaitée est saisie. Durant toute cette opération, une LED bleue est allumée jusqu'à la fin de l'enrôlement, avec un afficheur LCD qui affiche clairement les différentes étapes.

3.2.2 Système de contrôle d'accès

Une puce sur carte RFID permet d'ouvrir la porte, à l'aide d'un relais et d'une serrure. Lorsque la puce est correcte (relais excité), la serrure est ouverte et une LED verte s'allume ; sinon, le système émet un signal sonore via le buzzer et une LED rouge s'allume.

- **Remarque :**

Le pointage est effectué une seule fois par jour (pour le suivi disciplinaire des employés), tandis que l'accès est autorisé chaque fois que les employés quittent le département (pour des raisons de sécurité par rapport aux étrangers).

3.3 Schéma électronique complet du système

Fritzing est un logiciel open source dédié à la conception de circuits imprimés. Il offre une interface graphique intuitive permettant de concevoir et d'imprimer les typons des circuits de manière visuelle. Son objectif principal est de promouvoir le partage de circuits électroniques open source et d'aider à l'apprentissage de la conception de circuits.

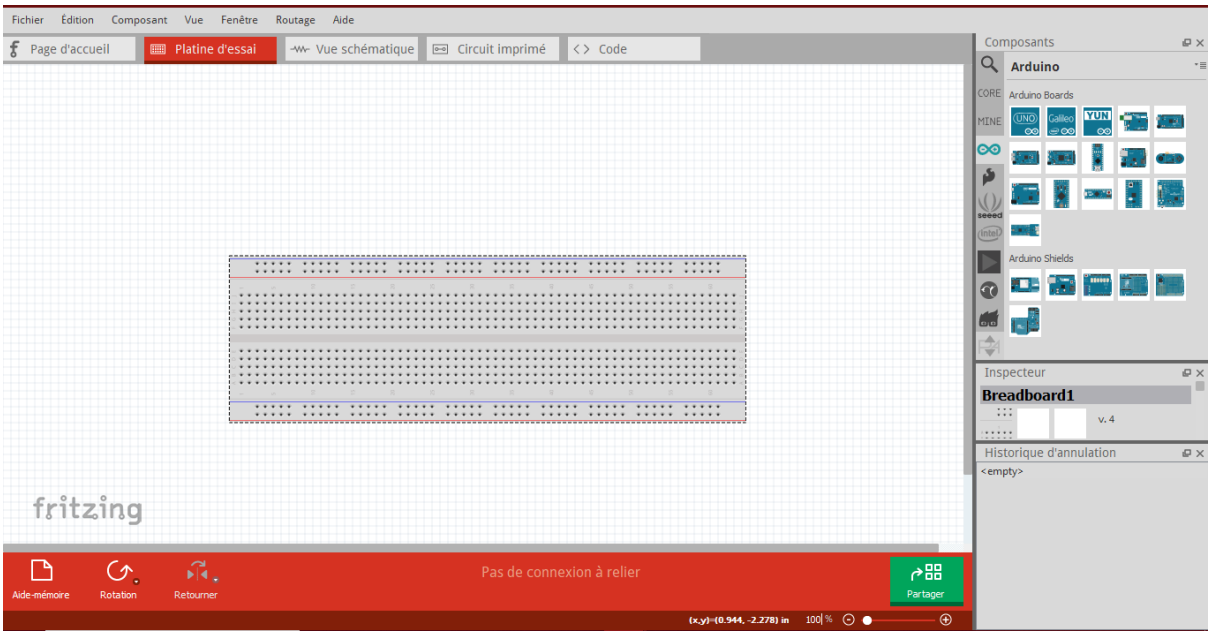


Figure 3. 1 : Environnement de travail du logiciel Fritzing.

Un schéma électronique créé avec Fritzing est une représentation visuelle des composants électroniques et de leurs connexions à une carte Arduino. Il utilise des symboles graphiques pour représenter la carte Arduino ainsi que les différents composants tels que les résistances, les capteurs, les LED, etc. Les connexions entre les composants sont illustrées par des lignes ou des fils qui indiquent comment les broches des composants sont connectées les unes aux autres ou à la carte Arduino. Des annotations peuvent être ajoutées pour fournir des détails supplémentaires sur les composants ou les connexions. En résumé, un schéma électronique Fritzing est un outil visuel utile pour comprendre la configuration électronique d'un projet Arduino et comment les différents éléments sont interconnectés.

3.3.1 Schéma électronique pour le pointage

La **figure 3.2** montre un montage électronique pour un système de pointage, détaillant les connexions entre capteurs, microcontrôleur et afficheur. Les symboles standardisés des composants permettent de comprendre rapidement le fonctionnement et les interactions du système, facilitant ainsi son analyse, sa mise en œuvre et son dépannage.

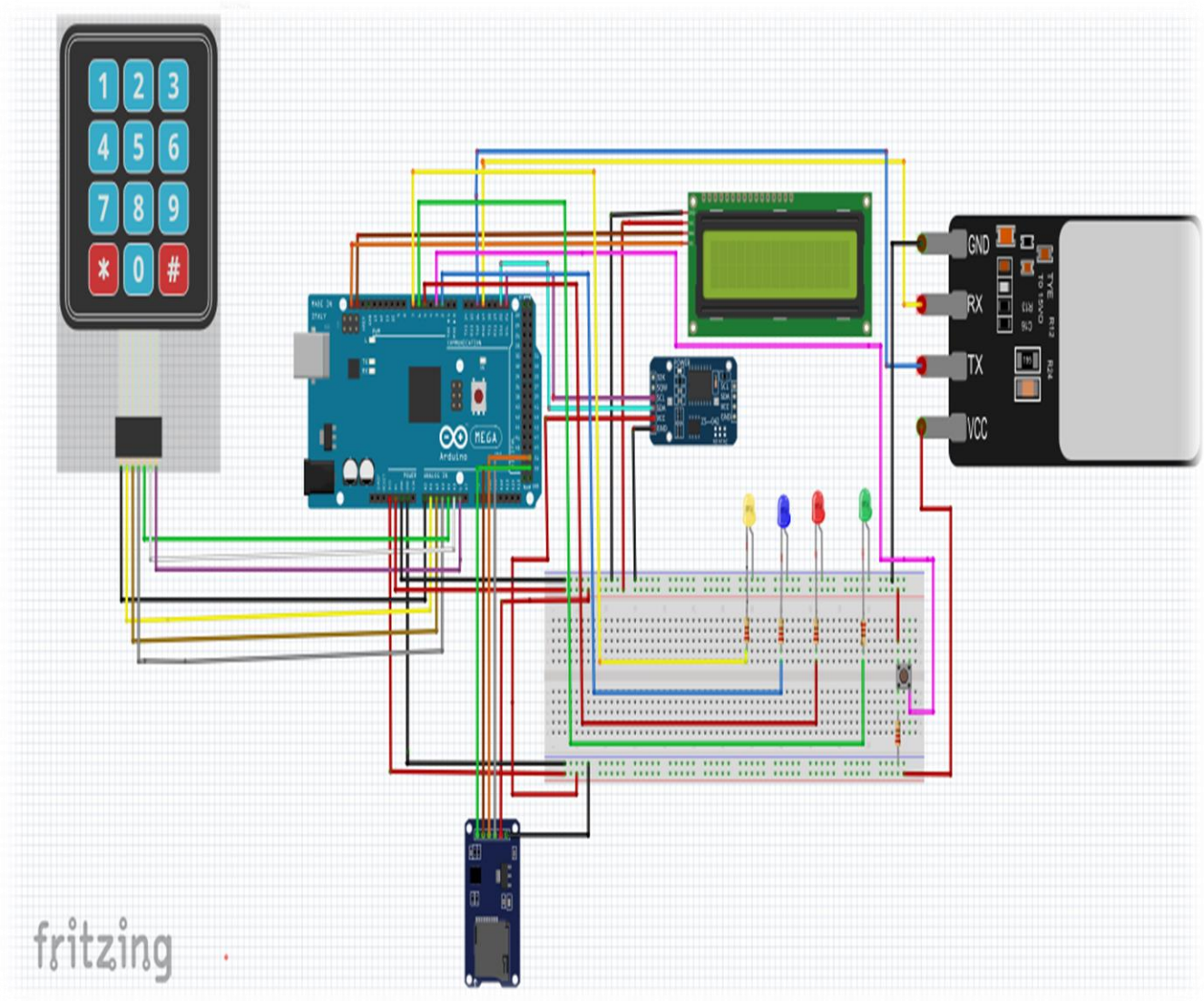


Figure 3. 2 : Branchement du système de pointage à l'aide du logiciel Fritzing.

3.3.2 Schéma électronique pour le contrôle d'accès

La **Figure 3.3** présente un montage électronique pour un système de contrôle d'accès, illustrant les connexions entre les capteurs, le microcontrôleur et les dispositifs de verrouillage. Grâce à l'utilisation de symboles standardisés, il est possible de comprendre facilement le fonctionnement et les interactions entre les différents composants. Cela simplifie l'analyse, l'installation et la maintenance du système de contrôle d'accès.

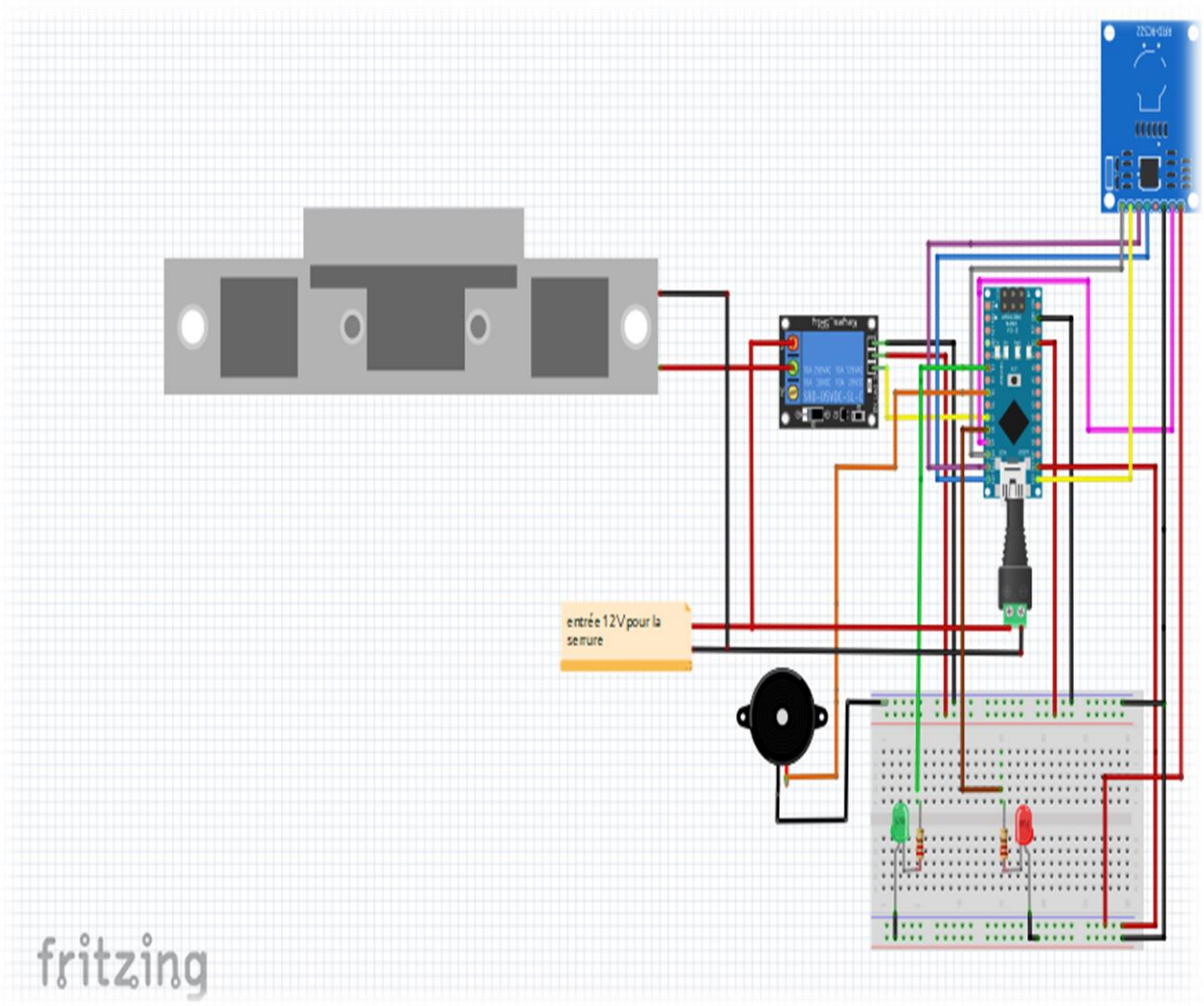


Figure 3. 3 : Branchement du système de contrôle d'accès à l'aide du logiciel Fritzing.

3.4 Branchement des composants

Le branchement des composants implique de connecter entre eux les différents éléments d'un système électronique ou électrique. Cela inclut la liaison soigneuse des capteurs, actionneurs, microcontrôleurs, relais et autres dispositifs selon un schéma précis, assurant ainsi que le système fonctionne de manière efficace et fiable. Chaque connexion est réalisée selon les spécifications techniques du circuit, garantissant une performance optimale dans l'exécution des fonctions prévues.

3.4.1 Branchement du système de pointage

Le tableau ci-dessous présente les broches de connexion essentielles pour un système de pointage, permettant de relier efficacement les capteurs, microcontrôleur et afficheur.

Tableau 3. 1 : Branchement du système de pointage avec Arduino Méga.

Module	***Nom de branche***	***Pin d' Arduino Méga***
Empreinte digitale	Vcc	3.3 V
	GND	GND
	RX	RX2 (D17/PWM)
	TX	TX2 (D16/PWM)
RTC	VCC	3.3 V
	GND	GND
	SDA	SDA D20
	SCL	SCL D21
SD Card	VCC	5V
	GND	GND
	CS	D53
	SCK	D52
	MOSI	D51
	MISO (MOSO)	D50
Clavier matriciel	1	A0
	2	A1
	3	A2
	4	A3
	5	A4
	6	A5
	7	A6
Bouton	Pin	D3/PWM
LED bleu	Pin	D2/PWM
LED rouge	Pin	D5/PWM
LED verte	Pin	D6/PWM
LED jaune	Pin	D7/PWM

3.4.2 Branchement du système de contrôle d'accès

Le tableau ci-dessous présente les broches de connexion essentielles pour un système de contrôle d'accès, permettant de relier efficacement les capteurs, microcontrôleur et afficheur.

Tableau 3. 2 : Branchement du système contrôle d'accès avec Arduino Nano.

Module	***Nom branche***	***Pin Arduino Nano***
RFID	VCC	3.3V
	GND	GND
	SCK	D13
	MISO	D12
	MOSI	D11
	SDA	D10
	RST	D9
Buzzer	Pin	D5
Relais	Pin	D7
LED verte	Pin	D3

.

3.5 Montage global du système pointage

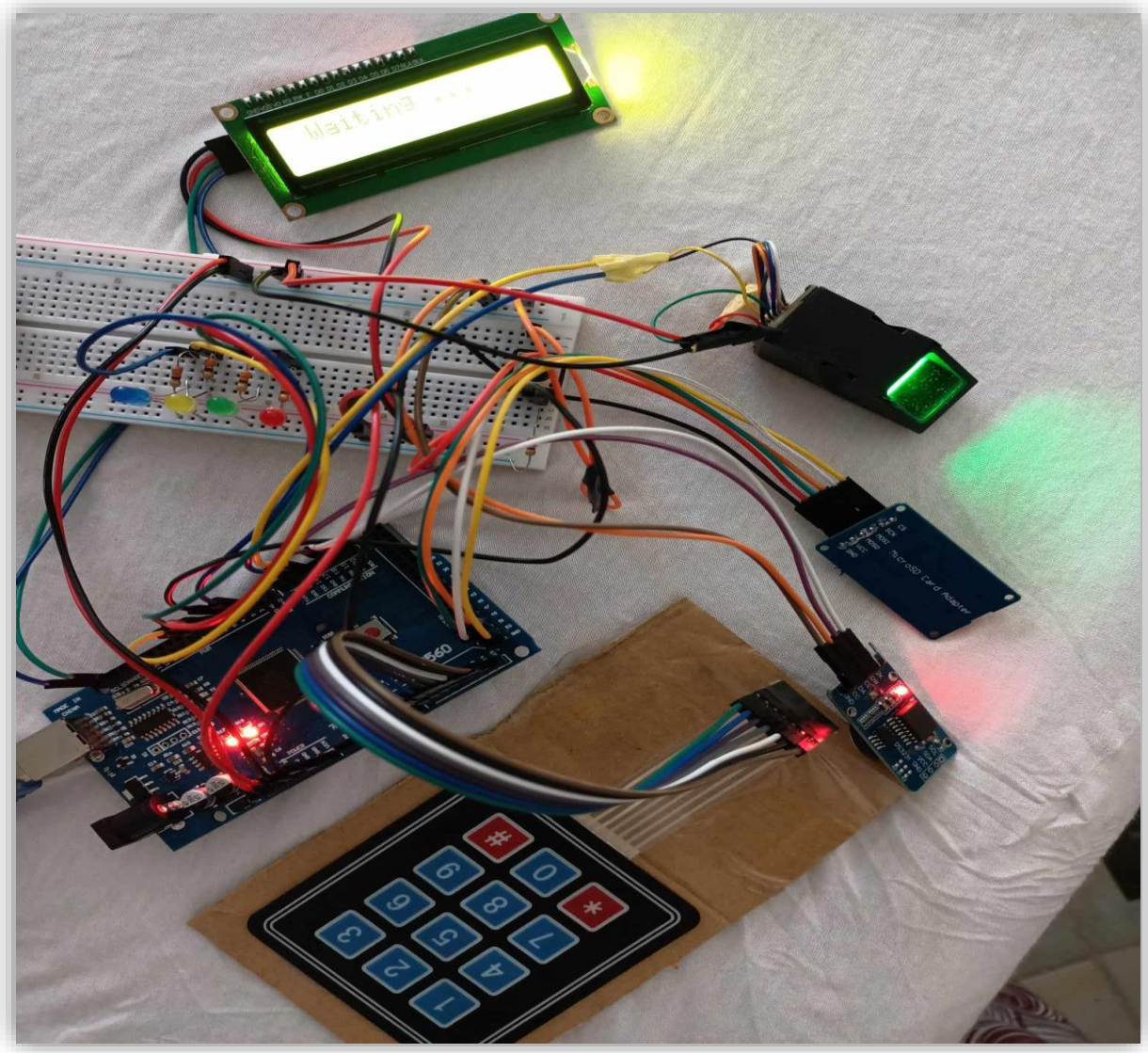


Figure 3. 4 : Montage global pour le système de pointage.

3.6 Montage globale du système de contrôle d'accès

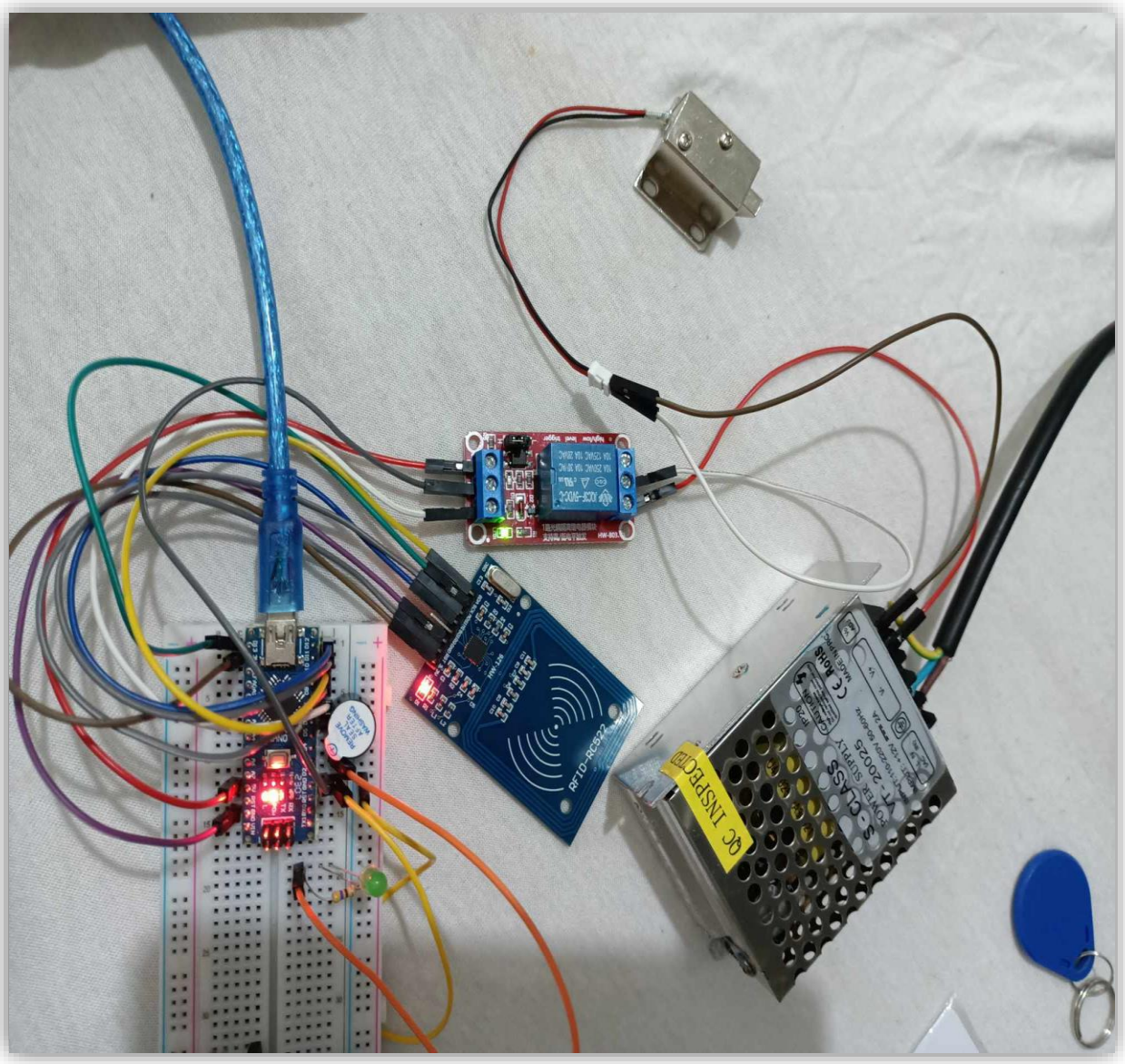


Figure 3. 5 : Montage global pour le système de contrôle d'accès.

3.7 Tests et interprétations

3.7.1 Système de pointage

Ce système se compose de deux parties essentielles : partie du pointage avec l'enregistrement des pointages des employés sur la carte SD et l'enrôlement des nouvelles données par la pression du bouton bleu.

- **Pointage**
  - Au début, l'afficheur LCD affiche « WELCOME » pour initialiser le système , après « Waiting » permettant d'insérer le doigt pour pointer:

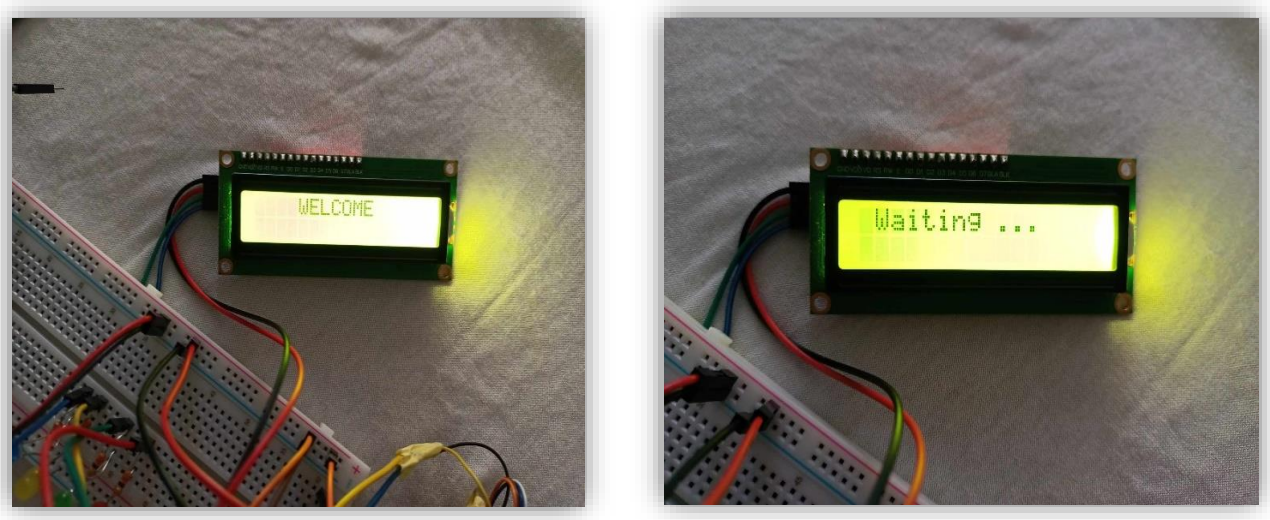


Figure 3. 6 : Affichage « WELCOME » et « Waiting » sur LCD.

- On pose le doigt nécessaire pour le pointage avec l'affichage du message « Converted » :

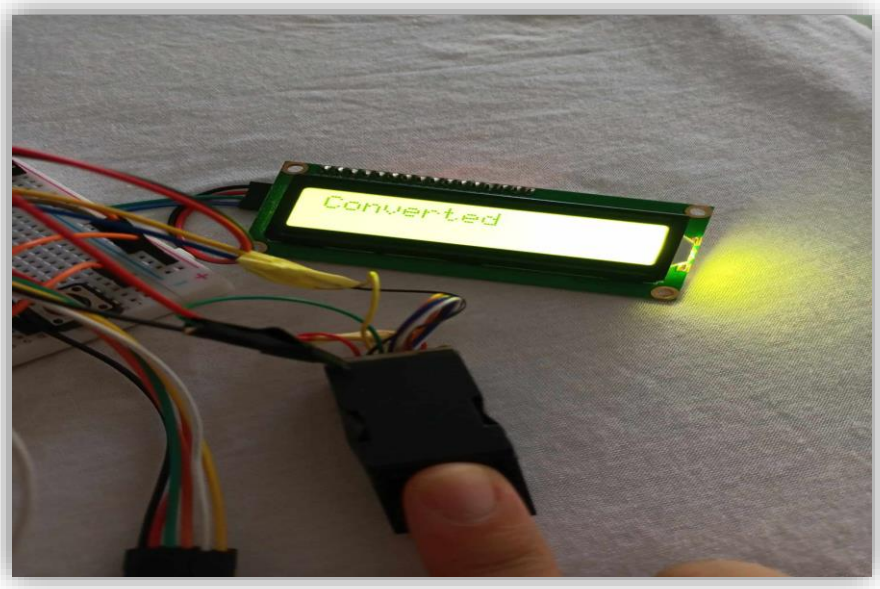


Figure 3. 7 : Affichage « Converted » sur LCD.

- Si l'employé n'existe pas sur la base de données, l'afficher va afficher « UNKNOWN ! » avec une LED rouge sera allumée.
- Si l'employé est connu et existe sur la base de données : le pointage est réussi avec l'affichage « SUCCES ! » l'allumage du LED verte.

  Le stockage des données du pointage après l'indication de la LED verte, sera enregistré sur la carte SD insérée au début du système.

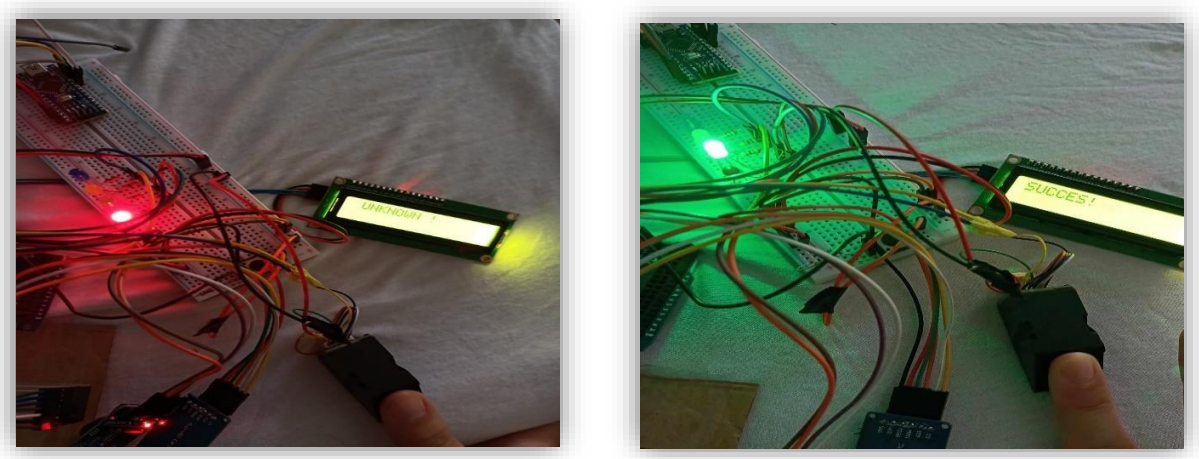


Figure 3. 8 : Résultat du système de pointage.

- Si le doigt n'est pas stable et bien posé sur le lecteur, une LED jaune sera allumée avec l'affichage du message « No fingerprint ».

➢ **Enrôlement de nouvelles empreintes à l'aide d'un bouton ;**

- Presser le bouton permet d'intégrer de nouvelles empreintes enregistrées sur la base de données et affichage du message « Enroll system » .

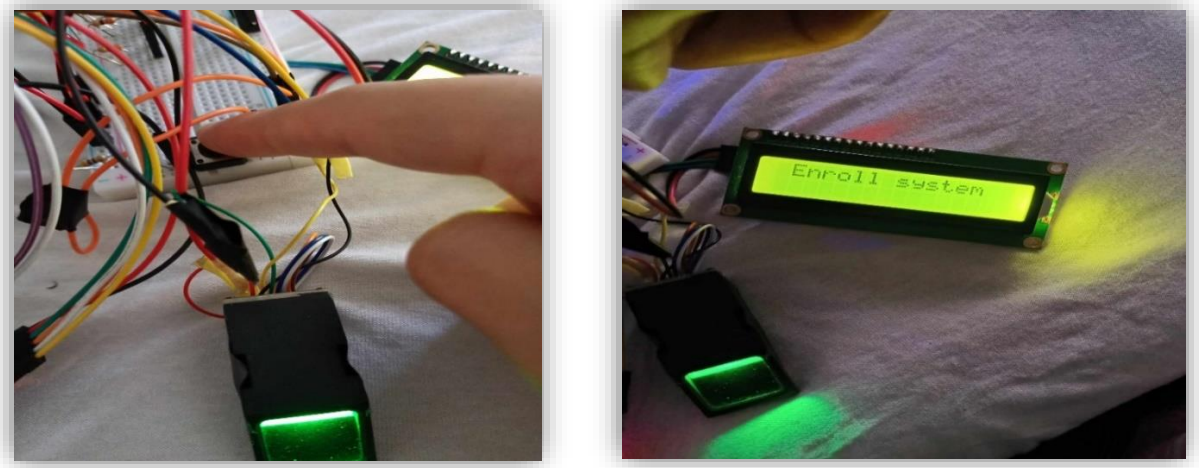


Figure 3. 9 : Pression sur le bouton pour commencer l'enrôlement.

- Demande d'un mot de passe matriciel pour accéder au système d'enrôlement « Enter Password » une LED bleue sera allumée durant toute l'opération.
- Apres l'insertion du mot de passe correcte « 1111 » affiché sur LCD « **** », il est nécessaire d'appuyer n'importe quelle touche sur le clavier comme si c'est un OK, par le message « Press any key to start enrollement ».

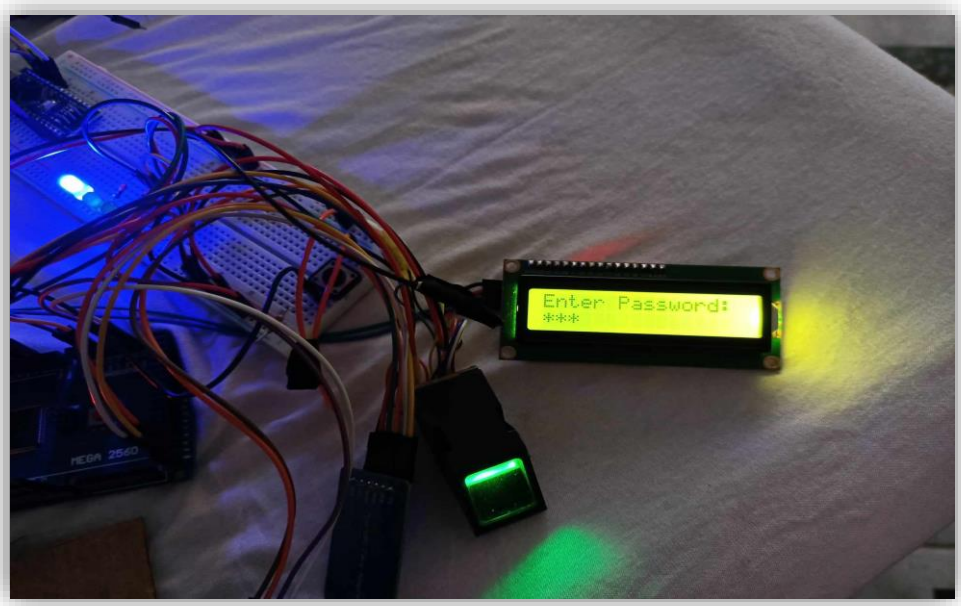
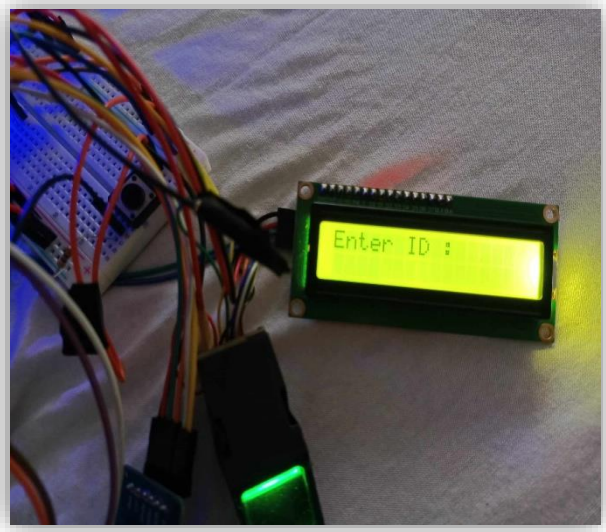


Figure 3. 10 : Insertion du mot de passe.

- Il faut entrer ID personnalisé par chaque employé par le clavier matriciel affichant pour cela le message « Enter ID » , pour un essai on a pris ID=5:



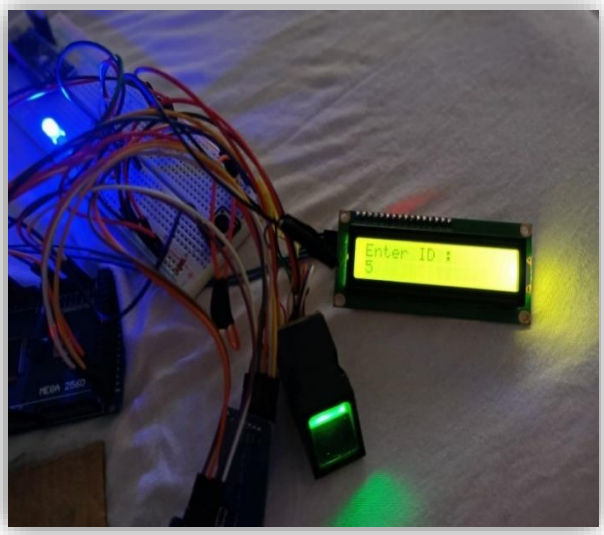


Figure 3. 11 : Entrer ID (ID=5).

- Commencer d'enregistrer l'empreinte par « put your finger », « remove your finger », « the same again », poser le doigt puis l'enlever et le poser encore une autre fois.
- Une fois que l'enrôlement est terminé, un message sera affiché « Image taken », « model created »

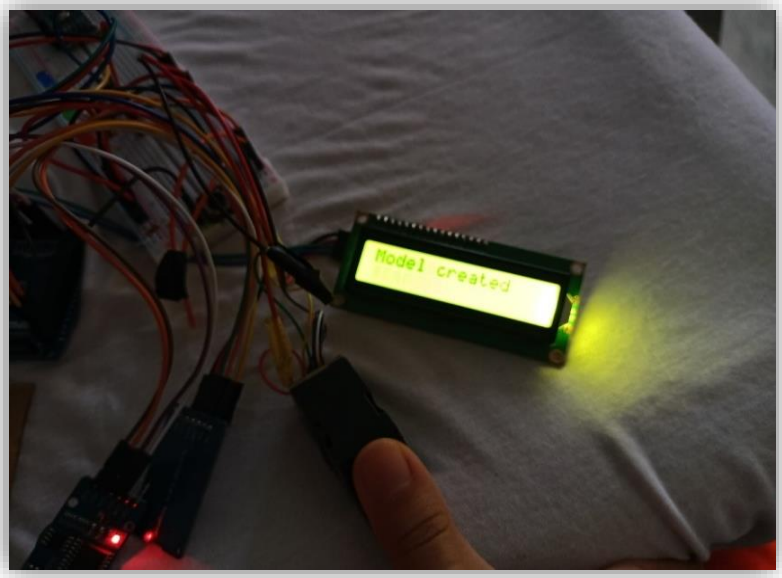


Figure 3. 12: Modèle crée.

- L'empreinte ajoutée (ID = 5), est à la base de données et l'employé peut pointer maintenant.

Remarque

Si le mot de passe est incorrecte, une LED rouge allumée avec l'affichage du message « INCORRECT » sur LCD.

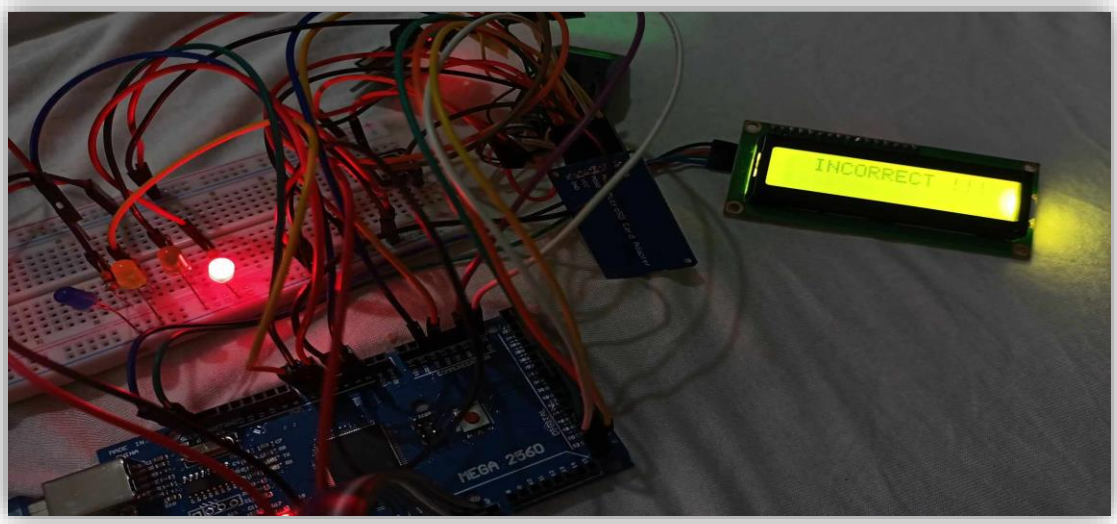


Figure 3. 13 : Affichage lors mot de passe incorrect.

- **Enregistrement sur carte SD ;**
  - Apres le retrait de la carte mémoire qui était installée sur le lecteur carte SD, à l'aide d'un adaptateur, on trouve un fichier texte nommé « POINTAGE ».

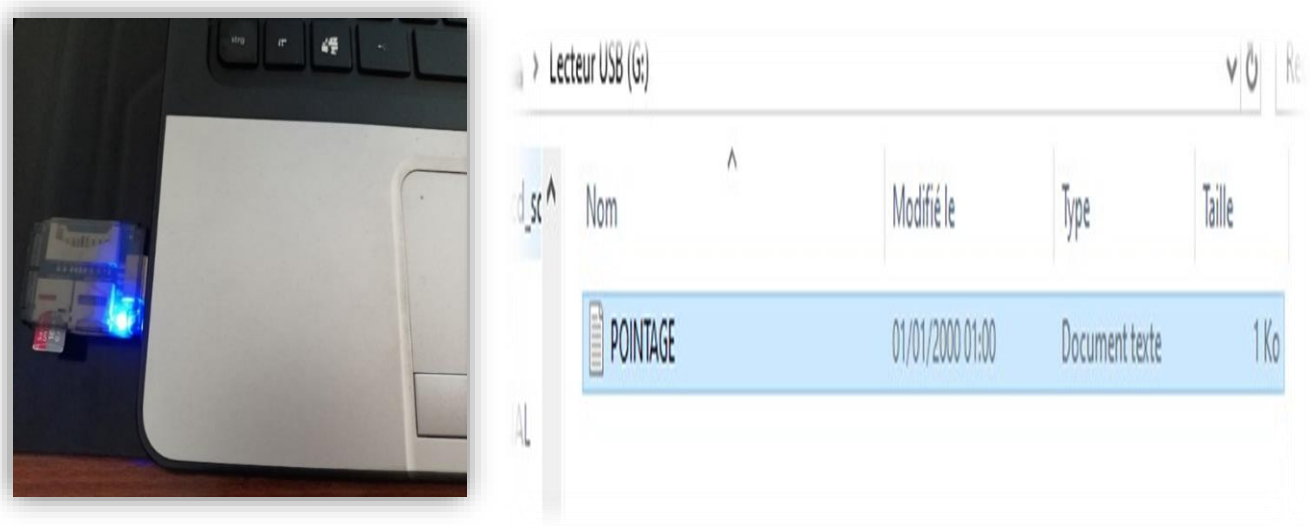


Figure 3. 14 : Adaptateur carte SD et fichier POINTAGE.txt.

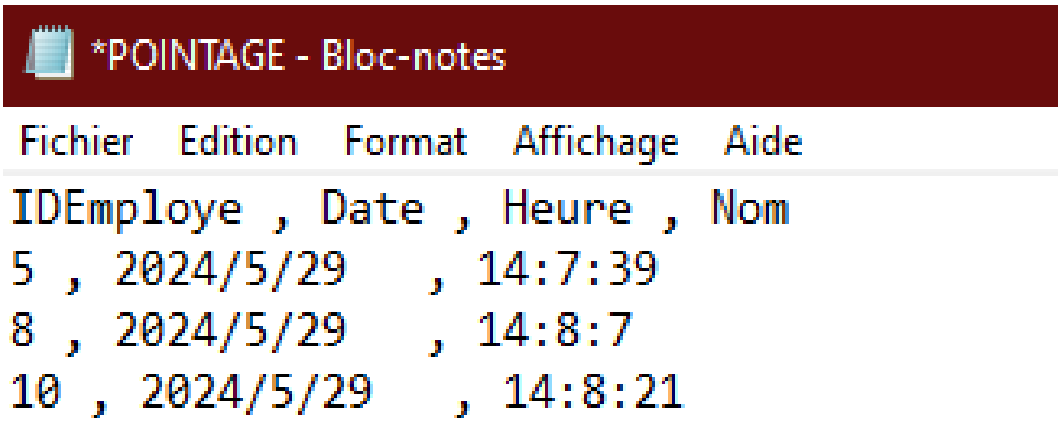


Figure 3. 15 : fichier texte du pointage.

- On ouvre ce fichier texte par excel par données externes :
- On utilise comme séparateur la virgule entre les colonnes.

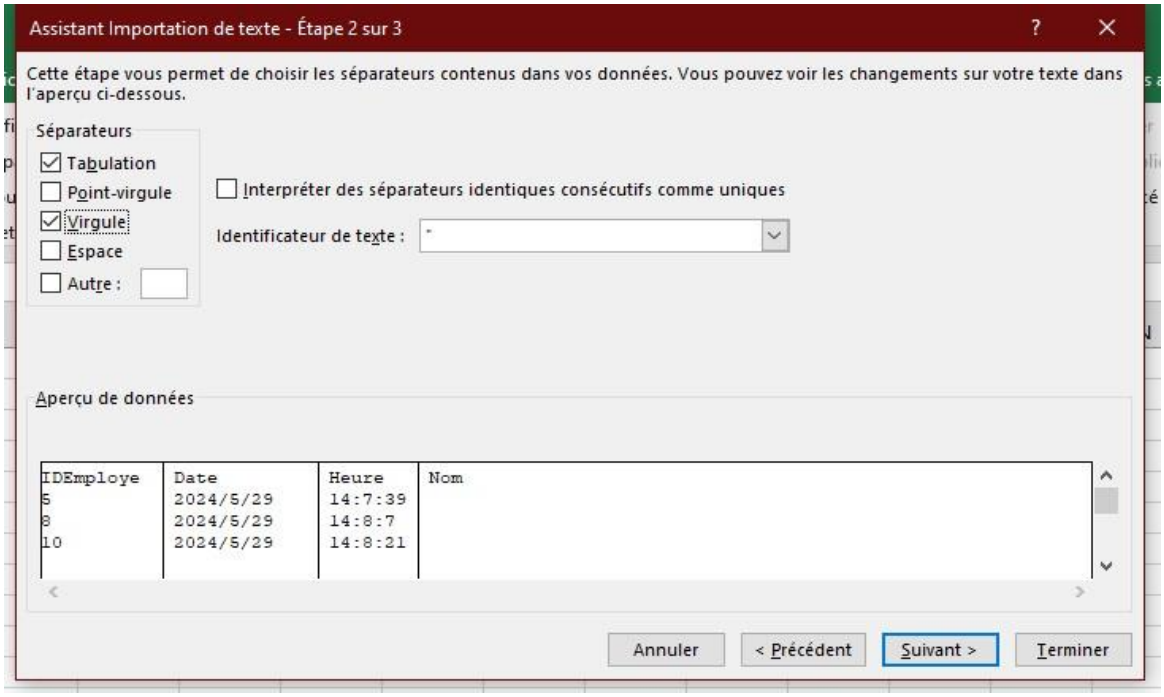


Figure 3. 16: Réglage sur Excel.

- **Remarque**

Pour la case du nom, on a utilisé les fonctions d'excel, en lui donnant une condition suivant le IDEmploye, pour que le nom sera automatique à chaque fois :

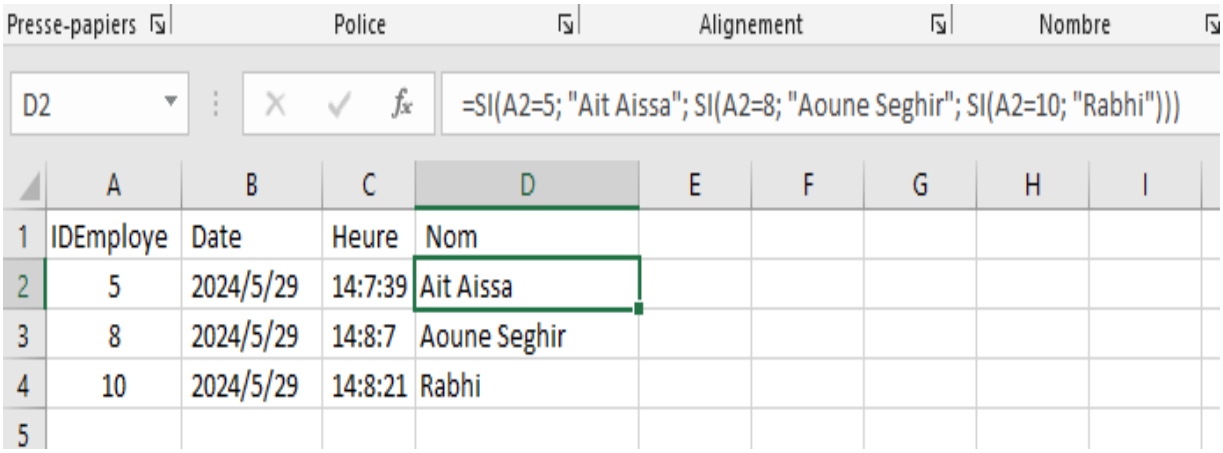


Figure 3. 17: Condition pour le nom sur Excel.

3.7.2 Système de contrôle d'accès

- Si on scanne la puce qui a le ID Card = « 53 3c de 99 » qui est enregistré sur la base de données, une LED verte sera allumée et la serrure s'ouvre :

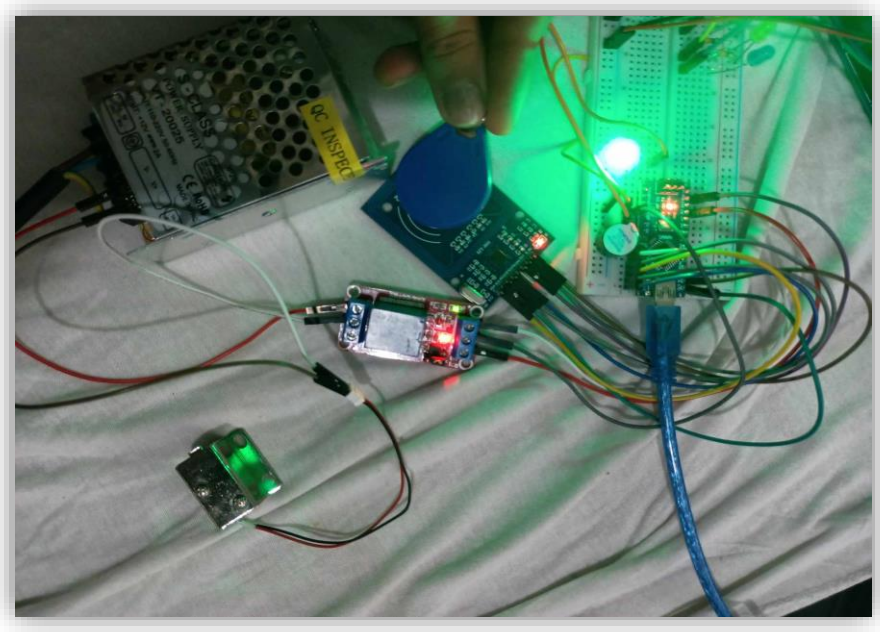


Figure 3. 18 : Ouverture de la serrure par la puce.

- Si on scanne la carte qui a le ID card = « 13 b2 8a 0e » qui n'existe pas sur la base de donnée, le buzz sonne, ce qui conclue la fermeture de la poste (la serrure reste au mode fermé (repos, initiale)) :

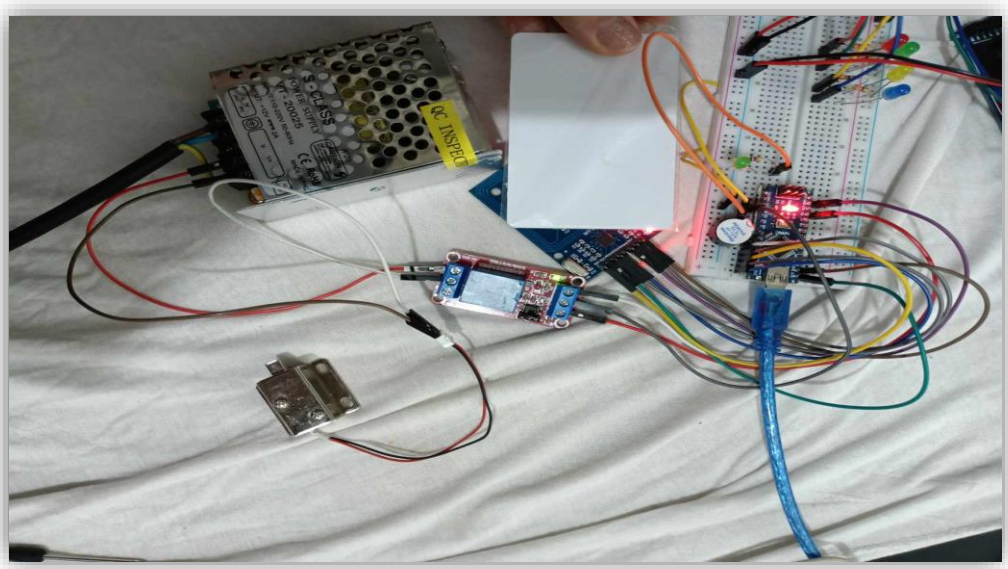


Figure 3. 19 : Fermeture de la serrure par la carte.

➢ **Résultats**

- Les LEDs sont des indicateurs visuels de l'état ou du fonctionnement d'un système. Dans notre système de pointage, nous avons utilisé quatre LEDs, chacune ayant son rôle spécifique :
  - LED rouge : indicateur mot de passe incorrect.
  - LED verte : pointage réussi.
  - LED jaune : position incorrecte du doigt sur le lecteur d'empreinte digitale.
  - LED bleue : début d'enrôlement suite d'une pression d'un bouton bleu.
- Pour le système de contrôle d'accès :
  - LED rouge et Buzzer : accès refusé pour l'ouverture de la porte.
  - LED verte : accès autorisé (ouverture de la porte).
- Lors du retrait de la carte SD de son lecteur, un message s'affiche « erreur SD » donc il est nécessaire de réinitialiser le système par un bouton reset.
- Les deux boutons rouges sont distingués pour un Reset pour les deux cartes Arduino.

3.8 Conclusion

En conclusion, la conception du système de pointage et de contrôle d'accès par empreinte digitale et carte RFID présentée dans ce chapitre pose les bases solides pour la réalisation et l'implémentation d'un système performant et sécurisé. Les étapes détaillées dans ce chapitre assurent une compréhension claire des aspects techniques et fonctionnels nécessaires pour la mise en œuvre réussie de ce projet innovant.

Conclusion générale

Ce système est conçu à l'aide d'Arduino, une plateforme reconnue pour sa fiabilité, sa puissance et son coût abordable. Ces caractéristiques permettent de rendre notre projet plus accessible et attractif pour ceux cherchant à sécuriser leurs banques, entreprises, voire leurs domiciles. En optant pour Arduino, nous nous appuyons sur une technologie largement répandue et éprouvée, ce qui facilite non seulement le développement, mais aussi la commercialisation de notre solution. Grâce à sa popularité et à la vaste communauté de développeurs qui l'entoure, Arduino offre un support et des ressources abondantes, simplifiant ainsi le processus de mise en œuvre et de dépannage.

Cette approche ouvre la voie à une adoption plus large de notre système, offrant des opportunités accrues pour répondre aux besoins de sécurité dans divers environnements. En intégrant des technologies de pointe comme l'empreinte digitale et la RFID avec une plateforme aussi accessible qu'Arduino, nous créons une solution innovante et efficace qui peut être rapidement déployée et adaptée aux exigences spécifiques de chaque utilisateur. De plus, l'utilisation d'Arduino permet de maintenir les coûts de production bas, ce qui est un avantage significatif pour les petites et moyennes entreprises ou les particuliers cherchant à améliorer leur sécurité sans investir des sommes considérables.

En conclusion, l'utilisation d'Arduino dans le développement de notre système de sécurité renforce non seulement l'efficacité et la fiabilité de la solution, mais elle assure également une adoption plus facile et plus rapide grâce à la familiarité et la confiance qu'inspire cette technologie. Cela garantit que notre solution peut répondre aux défis de sécurité modernes tout en restant accessible à un large éventail d'utilisateurs.

Bibliographie

[1] https://www.horloges-huchez.fr/blog/tout-savoir-sur-le-pointage.

[2] https://www.staffplanning.io/les-differents-systemes-de-pointages-en-entreprise.

[3] https://peoplespheres.com/fr/systeme-de-pointage-tout-ce-quil-faut-savoir/.

[4] F. Massicotte, *LA BIOMÉTRIE, SA FIABILITÉ ET SES IMPACTS SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE,Mémoire doctorat,* UNIVERSITÉ DU QUÉBEC À MONTRÉAL, Novembre 2007.

[5] *Techniques de contrôle d'acces par biométrie,* CLUSIF (Club de la Sécurité des systèmes d'Information), juin 2003.

[6] A. Chaari, *Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non Superviséee,* France : Anis Chaari : Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non Supervisée, THESE de doctorat. Université d'Evry Val d'Essonne-France et Université de la Manouba, 6 Octobre 2009.

[7] H.Ahmed, *"Identification des individus par la biométrie multimodale" Mémoire de Magister*, Oran: Université Mohamed Boudiaf, 2014.

[8] A. S.Zitouni, *"Authentification et identification biométrique des personnes par les empreintes palmaires " Mémoire de Master*, Ouargla: Université Kasdi Merbah, 2016.

[9] https://ok_corige__memoire_M2ELN_khadir_et_ramli_(pointage_par_empeinte_digitale).pdf .

[10] https://www.gendarmerie.interieur.gouv.fr/pjgn/institut-de-recherche-criminelle-de-la-gendarmerie-nationale/l-expertise-decodee/identification/les-empreintes-digitales-la-doyenne-des-preuves-scientifiques.

[11] L. L. e. M. C.L.Tisse, *Systèmes biométriques pour la vérification d'individu.exemple : iris,* juillet 2004.

[12] B. Ibtissam, *Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus,* 2016.

[13] Calais, *La RFID, Identification par radio fréquence,* 8 Novembre 2007.

[14] D. S. Nguyen, *Développement des capteurs sans fils basés sur les tags RFID uhf passifs pour la détection de la qualité des aliments. THESE du doctorat,* france: Université de Grenoble, 2013.

[15] D. g. d. G. E. F. Pierre GEORGET, *L'identification par Radio Fréquence, Principes et applications, version 4.01*, France: EPCglobal, mars 2004.

[16] https://www.paragon-id.com/fr/inspiration/history-radio-frequency-identification-technology.

[17] Y. Belaizi, *Etude et conception d'un capteur RFID passif en bande UHF : application à l'agroalimentaire*, Mai 2019.

[18] R. Kheddam, *Approches logicielles de sûreté de fonctionnement pour les systèmes RFID. Autre [cs.OH].*, France: Université de Grenoble, 2014.

[19] https://www.univbejaia.dz/xmlui/bitstream/handle/123456789/21479/M%C3%A9moire%202.pdf?sequence=1&isAllowed=y.

[20] I. S, *Contrôle automatique de niveau d'eau, mémoire de fin de cycle,* Abderrahmane Mira-Bejaia, 2019-2020.

[21] https://www.nextpcb.com/blog/arduino-nano-pinout.

[22] https://whadda.com/fr/produit/module-rtc-ds3231.

[23] https://youpilab.com/components/product/clavier-matriciel-3x4.

[24] B. Cottenceau, *Carte Arduino UNO, Microcontroleur ATMega328,* ISTIA (École Polytechnique de L'Université d'Angers-France), 2016-2017.

[25] http://wiki.labaixbidouille.com/index.php/%C3%89mission_de_donn%C3%A9es_(RTC)/R%%A9ception_et_affichage_des_donn%C3%A9es.

[26] https://www.upesy.com/blogs/tutorials/upesy-micro-sd-reader-module-documentation-version-latest?shpxid=34000d1a-2eba-4fed-990f-1457c201753a#.

[27] https://www.electricity-magnetism.org/fr/comment-fonctionne-une-serrure-magnetique/.

[28] https://www.arduino-france.com/tutoriels/ide-arduino-installation-et-utilisation/.

[29] https://www.unilim.fr/pages_perso/deneuville/docs/Info2PC/Cours4.pdf.

[30] https://www.redohm.fr/2014/12/arduino-les-librairies/.

[31] https://nerd-mobile.com/articles/cest-quoi-un-lecteur-dempreinte-digital-optique..

[32] https://theses.hal.science/tel-00002923/document.

[33] https://docplayer.net/237086156-Benoit-charlot-publications-september-2022.html#.

[34] https://elainnovation.com/rfid-active-vs-rfid-passive-quelles-differences/.

[35] https://sbedirect.com/fr/blog/article/comprendre-la-rfid-en-10-points.html.

[36] https://www.myrfidsolution.com/comment-fonctionne-un-systeme-rfid/.

[37] https://www.rfidfuture.com/fr/lf-hf-and-uhf-frequency-whats-the-difference.html.

[38] https://www.staffplanning.io/les-differents-systemes-de-pointages-en-entreprise.

[39] S.Benkhaira, *" Systèmes multimodaux pour l'identification et l'authentification biométrique " ,Mémoire Magister,* Skikda: Universite 20 aout 1955-Skikda, 2010.

[40] I.Benchennane, *"Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus" Thèse de Doctorat,* Oran: Thèse de Doctorat,Universite Mohamed Boudiaf , 2016.

[41] M. E. Abed, *"Evaluation de systemes biometriques Liming" Thèse de Doctorat,* Basse - Normadie: Universitecaen, 2011.

[42] S.Boudjella, *"Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus" Thèse de Doctorat,* Tizi-Ouzou: Universite Mouloud Mammeri.

[43] https://www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom12.html.

[44] https://www.flaticon.com/fr/icone-gratuite/rfid_5261633.

[45] https://www.researchgate.net/figure/Schema-illustrant-un-systeme-RFID-Les-etiquettes-sont-aussi-appelees-transpondeur-ou_fig1_283349710.

[46] https://www.univbejaia.dz/xmlui/bitstream/handle/123456789/21479/M%C3%A9moire%202.pdf?sequence=1&isAllowed=y.

[47] S.Boudjella, *"detection et identification de personne par méthode biométrique" Mémoire de Magister,* Tizi-Ouzou: Universite Mouloud Mammeri .

[48] http://ok_corige__memoire_M2ELN_khadir_et_ramli_(pointage_par_empeinte_digitale).pdf.