الجـــــــــــــــــــــــــــمـهـوريـــــــة الجـــــــــــــــزائـريـة الديمـــــــــقـراطيـة الـشـــــــــــعبيـة

**RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE**

وزارة التـــــــــــــــــــــــــــــعـليـم العـــــــالي والبـــــــــــــحث العـــــلـمـــي

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**جامعة محمد البشير الإبراهيمي – برج بوعريريج**

**Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj**

**Faculté des Sciences et de la Technologie**

**Département : Electronique**

# MÉMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

**En** : Télécommunications

**Spécialité** : Systèmes des télécommunications

**Présenté Par** : - Dahmouni Bessam

- Semouma Ahmed Wail

## Théme

*Système de Sécurité biométrique pour une Smart Home / M2M-IoT*

Soutenu publiquement, le 30 /06/2025 , devant le jury composé de :

| | | | |
|---|---|---|---|
| M.ATIA Salim | Prof. | **Univ-BBA** | Président |
| M.HAFDI Zakaria | MCB. | **Univ-BBA** | Examinateur |
| M.AIDEL Salih | Prof. | **Univ-BBA** | Encadreur |

Année Universitaire 2024/2025

# *Remerciements*

*Je tiens tout d'abord à exprimer ma profonde gratitude à Dieu Tout-Puissant, source de force et de persévérance tout au long de ce travail.*

*Mes sincères remerciements vont également au Professeur AIDEL Salih, pour sa disponibilité, son accompagnement, ses conseils précieux et ses orientations éclairées tout au long de la réalisation de ce mémoire.*

*Je remercie également l'ensemble des enseignants du département pour les connaissances qu'ils nous ont transmises durant tout notre parcours universitaire.*

*Un grand merci à ma famille pour son soutien moral, ses encouragements constants et sa patience, qui ont été essentiels dans l'accomplissement de ce projet.*

*Toute ma reconnaissance va aussi à mes amis et collègues pour leur aide, leurs remarques constructives et leur soutien tout au long de cette aventure académique.*

*Enfin, je tiens à remercier les membres du jury pour avoir accepté d'évaluer ce travail, ainsi que pour le temps et l'expertise qu'ils ont consacrés à l'étude de notre projet.*

# *Dédicace*

*À mes chers parents,*
*Pour leur amour inconditionnel, leurs sacrifices et leur soutien constant tout au long de ma vie.*

*À mes frères,*
*Pour leur présence rassurante et leurs encouragements précieux.*

*À mes fidèles amis,*
*Pour leur solidarité, leur écoute et les moments partagés tout au long de ce parcours.*

*À mon chat bien-aimé,*
*Pour sa douce compagnie, son calme apaisant, et sa présence réconfortante pendant les longues nuits de travail.*

*À tous ceux qui ont cru en moi,*
*Je dédie ce modeste travail avec toute ma reconnaissance et mon respect.*

***Bessam***

# *Dédicace*

*À mes parents,*

*Merci pour tout. Pour votre amour sans limite, pour vos encouragements dans les moments de doute, et pour votre présence, toujours discrète mais essentielle. Ce travail, c'est aussi le fruit de votre soutien.*

*À mes deux sœurs,*

*Vous êtes ma fierté et mon repère. Merci pour votre tendresse, vos sourires et votre confiance en moi, même quand je doutais.*

*À mes amis,*

*Pour tous les instants partagés, pour les discussions, les rires et les encouragements : vous avez rendu ce parcours plus beau.*

*À mes camarades d'université,*

*Merci pour l'entraide, les efforts collectifs, les révisions de dernière minute et les bons souvenirs. Ensemble, on a franchi bien des étapes.*

*Ce mémoire vous est dédié, avec toute mon affection et ma reconnaissance.*

***Ahmed***

## Résumé

Ce projet vise à concevoir un système de sécurité biométrique intelligent pour les maisons connectées, en s'appuyant sur l'intégration des technologies émergentes telles que l'IoT (Internet des Objets) et le M2M (Machine-to-Machine).
il repose sur l'utilisation de plusieurs composants électroniques interconnectés (capteur d'empreintes AS608, Arduino, clavier matriciel, capteur PIR, GSM SIM800L, servo-moteur, etc.) pour permettre une authentification sécurisée, une détection de mouvement, et l'envoi de notifications en temps réel (SMS, appels).
Le système peut également être contrôlé à distance via SMS. Ce projet met en œuvre à la fois des connaissances théoriques et pratiques, en combinant programmation embarquée, électronique et communication mobile pour renforcer la sécurité des habitations intelligentes.

**Mots clés :** maison intelligente, IoT, M2M, Arduino , capteur, Sécurité.

**ملخص :**

يهدف هذا المشروع إلى تصميم نظام أمان بيومتري ذكي خاص بالمنازل الذكية، اعتمادًا على دمج تقنيات حديثة مثل إنترنت الأشياء (IoT) والتواصل بين الآلات.(M2M)
يعتمد النظام على عدة مكونات إلكترونية مترابطة (حساس بصمةAS608 ،Arduino، لوحة مفاتيح رقمية، حساس حركةPIR ، وحدةGSM SIM800L ، محرك سيرفو ...)بهدف تحقيق مصادقة آمنة، كشف الحركة، وإرسال إشعارات فورية عبر الرسائل النصية والمكالمات الهاتفية.
يمكن أيضًا التحكم في النظام عن بُعد باستخدام رسائل .SMS يجمع هذا المشروع بين الجانب النظري والجانب التطبيقي من خلال البرمجة الإلكترونية، والاتصالات اللاسلكية، لرفع مستوى الأمان في المنازل الذكية.

**الكلمات المفتاحية :** المنزل الذكي ، انترنيت الاشياء، اردوينو ، المستشعر، الامن .

## Abstract

This project aims to design a smart biometric security system for connected homes, leveraging emerging technologies such as the Internet of Things (IoT) and Machine-to-Machine (M2M) communication.
The system uses several interconnected electronic components (AS608 fingerprint sensor, Arduino, 4x4 keypad, PIR motion detector, GSM SIM800L module, servo motor, etc.) to provide secure user authentication, motion detection, and real-time alerts via SMS and phone calls.
It also supports remote control via SMS commands. This project combines theoretical knowledge and practical implementation, integrating embedded programming, electronics, and mobile communication to enhance smart home security.
**Keywords**: smart home, IoT, M2M, Arduino, Sensor, Security.

# Sommaire

# Liste des figures

## Liste des tableaux

# Liste des Abréviations

M2M : Machine-to-Machine

IoT : Internet of Things (Internet des objets)

OC : Objet Connecté

MQTT : Message Queuing Telemetry Transport

XAP : Extensible Authentication Protocol (ou autres significations selon le contexte)

XMPP: Extensible Messaging and Presence Protocol

CoAP: Constrained Application Protocol

2G (GSM): 2nd Generation (Global System for Mobile Communications)

3G (UMTS): 3rd Generation (Universal Mobile Telecommunications System)

4G (LTE): 4th Generation (Long-Term Evolution)

5G: 5th Generation (cellular network technology)

FDMA: Frequency Division Multiple Access

TDMA: Time Division Multiple Access

CDMA: Code Division Multiple Access

IEEE: Institute of Electrical and Electronics Engineers

FHSS: Frequency-Hopping Spread Spectrum

RFID: Radio Frequency Identification

NFC: Near Field Communication

WSN: Wireless Sensor Network

WiFi: Wireless Fidelity

CPL: Courants Porteurs en Ligne (Power Line Communication)

RF: Radio Frequency

IR: Infrared

ICSP: In-Circuit Serial Programming

USB: Universal Serial Bus

AC: Alternating Current

DC : Direct Current

# Introduction Générale

Dans un monde de plus en plus connecté, la sécurité des habitations devient une préoccupation majeure. L'évolution rapide des technologies numériques a permis l'émergence des maisons intelligentes (Smart Homes), où les objets interagissent de manière autonome pour assurer confort, efficacité énergétique et surtout, sécurité.

Pourtant, malgré les avancées dans le domaine de la domotique, la majorité des systèmes de sécurité domestique restent vulnérables aux intrusions et aux usurpations d'identité, notamment en raison de l'usage de méthodes d'authentification classiques (clés, badges, codes PIN). Ces méthodes, bien qu'accessibles, ne garantissent pas un niveau de sécurité optimal dans un environnement numérique exposé à des risques croissants.

Parmi les solutions les plus innovantes dans ce domaine, l'intégration des technologies biométriques dans les systèmes de sécurité offre un niveau de protection élevé en s'appuyant sur des caractéristiques uniques de l'individu, comme les empreintes digitales.

Le présent mémoire s'inscrit dans cette dynamique, avec la réalisation d'un système de sécurité biométrique pour maison intelligente, reposant sur les technologies IoT et M2M. Il s'agit d'un système embarqué capable de :

reconnaître les utilisateurs via un capteur d'empreintes digitales,

contrôler l'accès avec un clavier et un servo-moteur,

détecter les intrusions à l'aide d'un capteur de mouvement,

notifier le propriétaire en temps réel par SMS et appel grâce à un module GSM.

Ce projet se divise en trois chapitres principaux :

Le premier chapitre présente les concepts théoriques liés à l'IoT et au M2M, ainsi que leur application dans les systèmes de sécurité intelligents.

Le deuxième chapitre est dédié à la présentation des composants matériels utilisés et à l'analyse de leurs caractéristiques techniques.

Le troisième chapitre décrit la mise en œuvre pratique du système, l'implémentation logicielle, les tests réalisés ainsi que l'analyse des résultats obtenus.

À travers ce travail, nous visons à démontrer la faisabilité d'un système de sécurité intelligent, autonome et accessible, tout en proposant des perspectives d'amélioration et d'évolution vers des solutions encore plus performantes.

# CHAPITRE I :

## Les Principes Fondamentaux du M2M /IoT

# I.1 Introduction

Dans ce premier chapitre, nous présentons les concepts fondamentaux des technologies **M2M (Machine to Machine)** et **IoT (Internet of Things)**, qui sont à la base de notre système de sécurité intelligent.

# I.2 La communication M2M

## I.2.1 Définition de M2M

La communication M2M désigne l'échange automatisé de données entre des appareils (machines, capteurs, objets connectés) sans intervention humaine directe. Elle repose sur des technologies sans fil ou filaires pour permettre aux systèmes de communiquer, de collecter et de traiter des informations en temps réel [1].

## I.2.2 Historique du M2M

L'évolution de la communication M2M s'étend sur plusieurs décennies, marquée par des avancées technologiques majeures. Entre 1920 et 1960 - Figure1 -, les premières formes de M2M apparaissent avec le développement de la télémétrie, utilisée pour la surveillance à distance, et des systèmes SCADA dans le domaine de l'automatisation industrielle. Durant les années 1980 à 1990 - Figure1 -, l'émergence des protocoles industriels, tels que Modbus, facilite l'interconnexion des machines, tandis que les premières connexions sans fil via les réseaux 2G ouvrent la voie à une connectivité plus flexible. Dans les années 2000, la standardisation IP permet une meilleure intégration des systèmes, renforcée par la montée en puissance de la 3G, qui favorise le développement d'applications comme le suivi GPS ou la télérelève. La décennie 2010 marque une phase de convergence avec l'Internet des Objets (IoT), l'informatique en nuage (cloud), et les réseaux 4G/5G, entraînant une

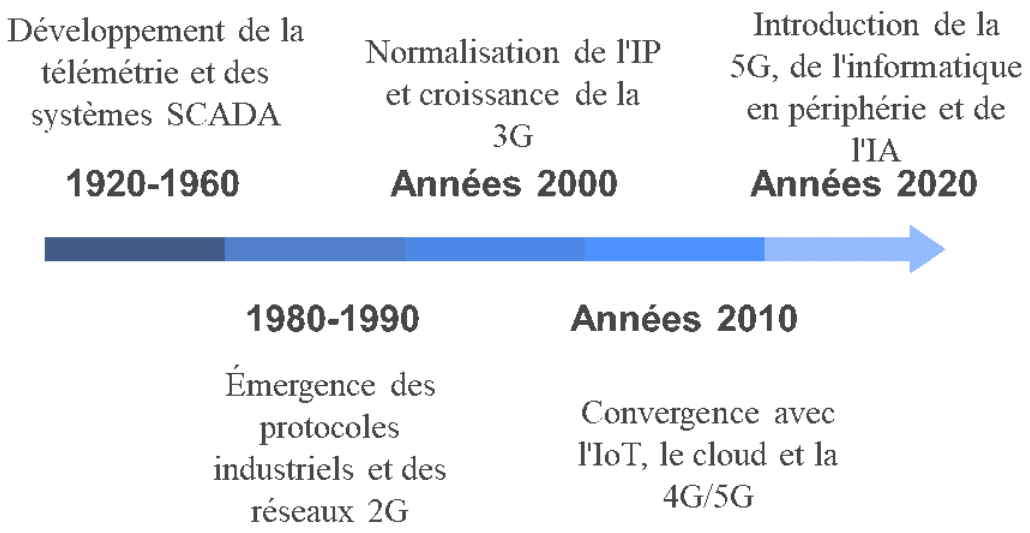



Figure 1:L'Historique du M2M.

explosion des usages dans des domaines variés tels que les villes intelligentes et l'industrie 4.0. Depuis les années 2020, l'introduction de la 5G, du edge computing et de l'intelligence artificielle a permis le développement d'applications ultra-connectées, comme les véhicules autonomes ou les dispositifs médicaux intelligents. À l'avenir, les perspectives se tournent vers la 6G et des réseaux M2M encore plus intelligents, autonomes et intégrés dans tous les aspects de la vie numérique [2].

### I.2.3 Caractéristiques principales du M2M

La communication M2M se distingue par plusieurs caractéristiques clés qui en font une technologie centrale dans les systèmes intelligents actuels. Tout d'abord, elle permet une automatisation complète des échanges de données, sans nécessiter d'intervention humaine pour initier ou gérer la communication. Elle repose ensuite sur une forte connectivité, utilisant divers types de réseaux, qu'ils soient sans fil (Wi-Fi, Bluetooth, 4G/5G, LoRa) ou filaires (Ethernet), afin d'assurer une transmission fluide et continue des informations. Intégrée dans les écosystèmes de l'Internet des Objets (IoT), la communication M2M contribue à l'interconnexion d'objets intelligents capables de collecter, traiter et échanger des données de manière autonome. Enfin, elle est particulièrement adaptée aux applications en temps réel, notamment dans les domaines de la

surveillance, du contrôle à distance et de l'analyse de données, ce qui renforce son rôle dans l'optimisation des processus industriels et des services connectés [3].

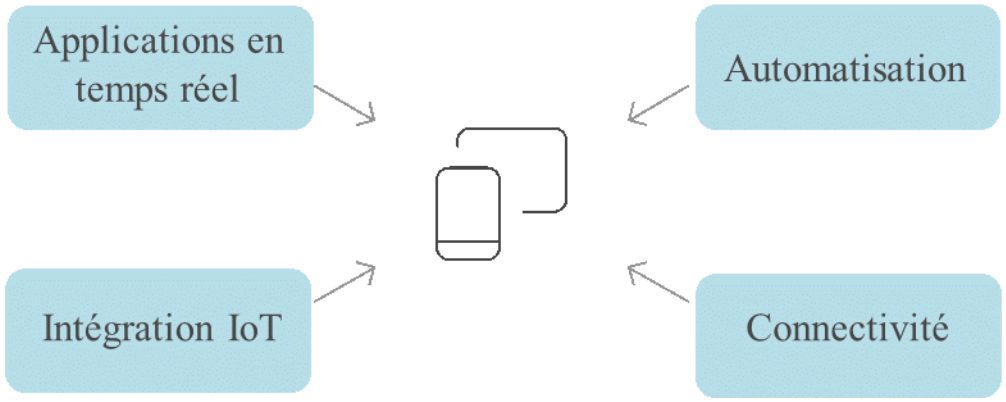



Figure 2 : Caractéristiques principales du M2M

### I.2.4 Fonctionnement du Réseau M2M

Le réseau M2M permet à des machines, capteurs ou équipements de communiquer automatiquement entre eux**,** sans intervention humaine, en s'appuyant sur des protocoles normalisés et des infrastructures spécifiques**.** Ce type d'architecture est conçu pour assurer un échange de données rapide, autonome et fiable, essentiel dans les environnements industriels,

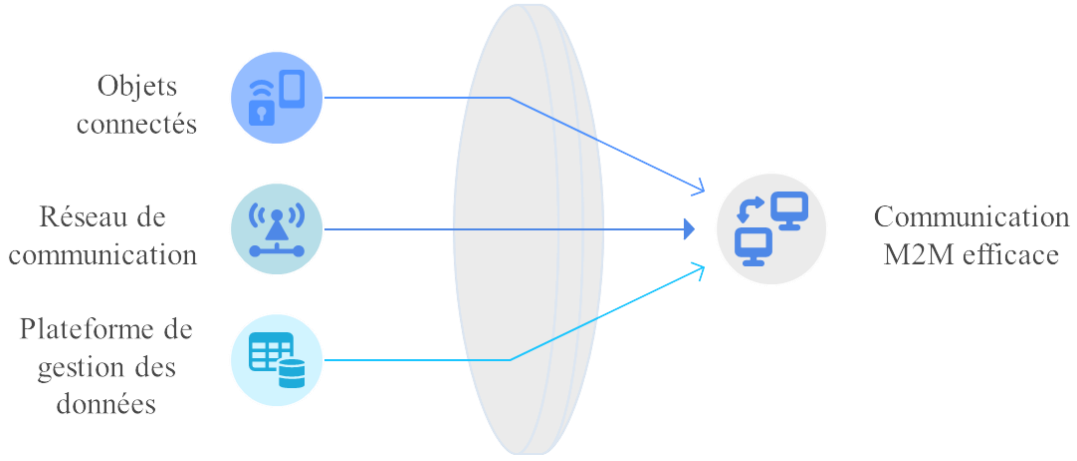



Figure 3 : Fonctionnement du Réseau M2M

urbains ou médicaux. Le fonctionnement d'un réseau M2M repose généralement sur trois composantes principales : les objets connectés, le réseau de communication et la plateforme de gestion des données [1].

### 1. Les Objets Connectés (Devices)

Cette première couche est constituée de capteurs (par exemple de température, d'humidité ou de mouvement), d'actionneurs (comme des moteurs, interrupteurs ou vannes), ainsi que d'équipements industriels plus complexes tels que des robots ou des machines-outils. Ces dispositifs ont pour rôle de collecter des données ou d'exécuter des actions en réponse à des signaux reçus. Un exemple concret est le compteur intelligent Linky, qui envoie automatiquement des données de consommation électrique au fournisseur d'énergie [1].

### 2. Le Réseau de Communication

La transmission des données entre les objets connectés et les systèmes centraux s'effectue via un réseau de communication qui peut être filaire (comme Ethernet, RS-485 ou PLC – Power Line Communication**) ou** sans fil **(**tels que les réseaux 2G/3G/4G/5G**,** NB-IoT**,** LoRaWAN**,** Sigfox, Wi-Fi ou Bluetooth). Ces communications sont encadrées par des normes reconnues, notamment :

- **3GPP** : pour les réseaux cellulaires adaptés aux communications M2M
- **IEEE 802.15.4** : pour les réseaux maillés comme Zigbee**,** utilisés dans les environnements à faible consommation énergétique [1].

### 3. La Plateforme de Gestion des Données (Backend)

Une fois les données transmises, elles sont traitées, analysées et stockées via des plateformes dédiées. Ces plateformes peuvent inclure des services de cloud computing (tels que AWS IoT**,** Microsoft Azure IoT**,** ou Google Cloud IoT), des systèmes SCADA (Supervisory Control and Data Acquisition) pour la surveillance industrielle, ou encore des middleware M2M comme OM2M, développé selon les standards de l'ETSI [1].

## I.3 L'Internet des objets IoT

### I.3.1 Définition de l'Internet des objets IoT

La définition de l'IoT selon l'Union Internationale des Télécommunications(UIT)est la suivante :

Une infrastructure mondiale pour la société de l'information, permettant la fourniture de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables, existantes ou en cours de développement

On peut également définir **l'Internet des Objets (IoT)** comme :

Un réseau qui connecte et intègre des objets à Internet, en suivant des protocoles assurant leur communication et l'échange d'informations à travers une variété de dispositifs [1].

### I.3.2 Historique de l'Internet des Objets (IoT)

L'Internet des Objets (IoT) s'est développé progressivement au fil des décennies, à la croisée des évolutions technologiques dans la communication, l'informatique et l'électronique. Son historique peut être divisé en plusieurs grandes phases :

**1. Origines (années 1800–1960)**

Les prémices de l'IoT remontent à des découvertes fondamentales en télécommunication. En 1832, le télégraphe électrique marque la première transmission de données à distance. Plus tard, en 1926, Nikola Tesla anticipe un système de communication sans fil entre objets. Enfin, en 1969, la création de l'ARPANET, ancêtre d'Internet, jette les bases des futurs réseaux interconnectés [4].

**2. Période pré-IoT (années 1980–1990)**

Durant cette période, plusieurs expérimentations annoncent l'IoT. En 1982, un distributeur de Coca-Cola est connecté à ARPANET pour signaler son stock — considéré comme le premier objet connecté. En 1990, John Romkey conçoit un grille-pain connecté à Internet, premier exemple d'objet domestique interactif. En 1999, Kevin Ashton, chez Procter & Gamble, introduit officiellement le terme "Internet of Things" [4].

### 3. Émergence (années 2000–2010)

Les premiers objets connectés grand public font leur apparition. En 2000, LG commercialise un réfrigérateur connecté. En 2008, le lancement de l'iPhone 3G rend les technologies mobiles et connectées accessibles au grand public. En 2009, Google expérimente les premières voitures autonomes, amorçant le développement des smart cities [4].

### 4. Expansion massive (2010–2020)

La décennie suivante est marquée par une explosion des usages. En 2011, le protocole MQTT, léger et optimisé pour les objets connectés, devient une norme majeure. En 2014, l'Amazon Echo (Alexa) démocratise la maison connectée. En 2016, le déploiement du NB-IoT, un réseau à faible consommation énergétique, étend l'IoT aux environnements contraints. En 2020, le monde compte plus de 30 milliards d'objets IoT, couvrant les domaines de la santé, de l'agriculture, de l'industrie ou encore des transports [4].

### 5. Perspectives futures (2020–2030+)

L'avenir de l'IoT repose sur des technologies encore plus puissantes et durables. Les réseaux 5G et 6G promettent une ultra-connectivité pour les applications critiques, notamment médicales ou autonomes. Parallèlement, l'intégration de l'intelligence artificielle et du edge computing permet un traitement local des données, réduisant la dépendance au cloud. Enfin, la notion d'IoT durable gagne en importance, avec un accent mis sur les énergies vertes, la sobriété énergétique, et le recyclage des dispositifs connectés [4].

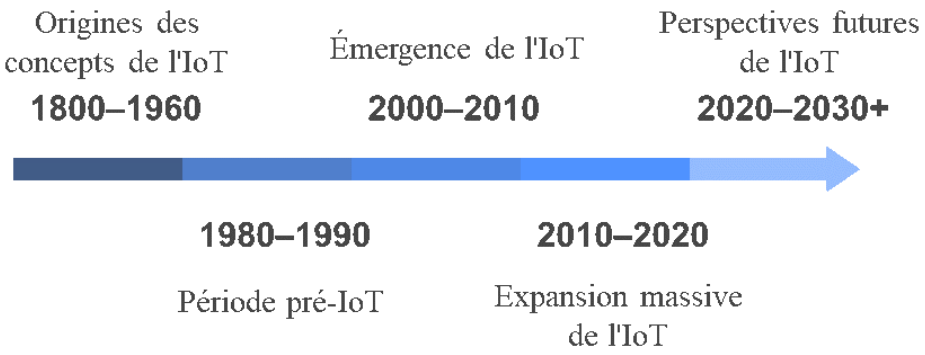



Figure 4 : l'Historique de lOT

### I.3.3 Fonctionnement du Réseau IoT

Le réseau IoT repose sur un écosystème d'objets physiques interconnectés capables de collecter, transmettre et traiter des données via Internet. Ces objets peuvent être des capteurs, des machines ou des appareils, intégrés dans différents environnements (domestique, industriel, urbain, médical). Le fonctionnement de l'IoT s'appuie sur une architecture en couches, permettant une modularité et une évolutivité du système [5].

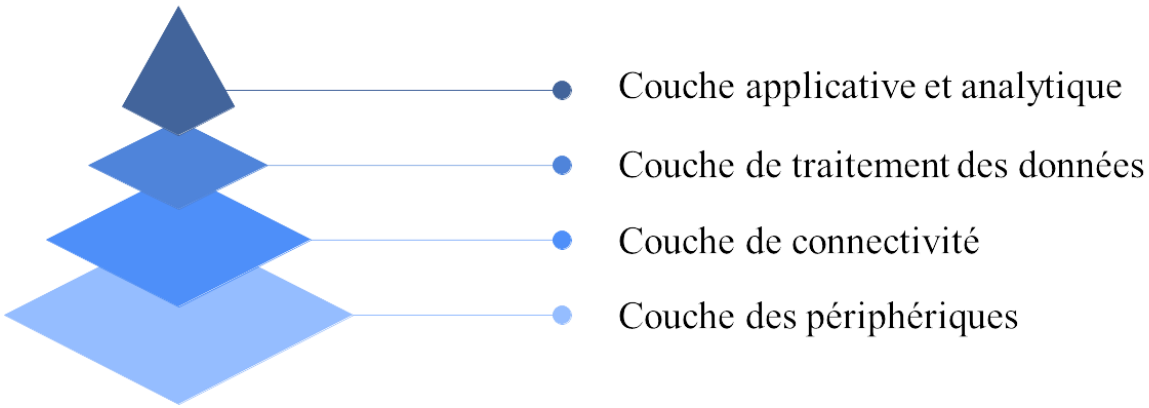



Figure 5 : Fonctionnement du Réseau IoT

**1. Couche des périphériques (Devices et Capteurs)**

Cette première couche concerne les objets connectés chargés de collecter des données physiques telles que la température, l'humidité, le mouvement ou la géolocalisation. Elle comprend :

- Des capteurs environnementaux (ex. : DHT22, capteurs LoRaWAN),
- Des dispositifs portables (wearables) comme les montres intelligentes ou les pacemakers,
- Des caméras intelligentes intégrant des fonctions de détection ou de reconnaissance [5].

**2. Couche de connectivité (Réseaux de communication)**

Cette couche assure la transmission des données collectées vers les plateformes de traitement. Les technologies utilisées varient selon les besoins en portée, débit et consommation énergétique :

- Technologies sans fil basse consommation : LoRaWAN, Sigfox, NB-IoT.
- Technologies à courte portée : Bluetooth Low Energy, Zigbee, Wi-Fi HaLow.
- Technologies longue portée et haut débit : LTE-M (4G), 5G.

Des protocoles de communication spécifiques sont également utilisés :

MQTT (Message Queuing Telemetry Transport), léger et optimisé pour les petits volumes de données,

CoAP (Constrained Application Protocol), une alternative au protocole HTTP, standardisé par l'IETF (RFC 7252) [5].

**3. Couche de traitement des données (Edge Computing et Cloud)**

- Les données transmises sont ensuite traitées, analysées et stockées via deux approches complémentaires :
- Edge computing : traitement local sur des dispositifs embarqués (ex. : NVIDIA Jetson), permettant de réduire la latence et d'améliorer la réactivité.
- Cloud IoT : traitement à distance sur des plateformes comme AWS IoT, Google Cloud IoT ou Azure IoT Hub, adaptées à l'analyse à grande échelle.
- Des middleware open source, tels que FIWARE ou ThingsBoard, assurent l'orchestration entre les objets et les services de traitement [5].

**4. Couche applicative et analytique**

Enfin, les données traitées sont utilisées dans des applications concrètes, via :

- Des dashboards de visualisation (ex. : Grafana, Power BI),
- Des algorithmes d'intelligence artificielle et de machine learning pour la détection d'anomalies ou la maintenance prédictive,
- Des mécanismes d'automatisation, comme l'activation d'un système d'arrosage en cas de sol sec.

Cette couche représente la finalité du système IoT, transformant les données collectées en actions utiles, visibles et exploitables [5].

## I.4 Différence entre M2M et IoT

Bien que souvent associés, les concepts de Machine-to-Machine (M2M) et d'Internet des Objets (IoT) présentent des différences fondamentales en termes d'architecture et de finalité. Le M2M se concentre principalement sur la communication directe entre machines, en utilisant des protocoles

dédiés et des connexions souvent point à point. Il permet l'échange d'informations automatisé entre dispositifs sans nécessairement passer par Internet, ce qui le rend particulièrement adapté aux environnements industriels [6].

En revanche, l'IoT va au-delà de cette simple communication en connectant les objets à Internet, permettant ainsi une gestion centralisée des données via des plateformes cloud et des outils d'analyse massive (big data). Cette centralisation facilite l'optimisation des processus, le déploiement d'intelligence artificielle et le contrôle à distance à grande échelle [6].

En résumé, le M2M constitue un socle technologique essentiel, favorisant l'automatisation et l'efficacité dans de nombreux secteurs, tandis que l'IoT représente une évolution globale de ce modèle, intégrant des couches de connectivité, de traitement et de services orientés vers une interopérabilité étendue et une intelligence distribuée [6].

## I.5 Applications du M2M et de l'IoT dans la vie quotidienne

Les technologies M2M (Machine-to-Machine) et IoT (Internet des Objets) sont aujourd'hui largement intégrées dans de nombreux domaines de la vie quotidienne. Elles permettent d'automatiser des tâches, améliorer l'efficacité des services, et offrir un meilleur confort aux utilisateurs. Voici quelques exemples concrets d'applications :

### 1. Santé connectée

Les dispositifs connectés jouent un rôle croissant dans la prévention et le suivi médical :

- Les montres intelligentes et bracelets de santé permettent de surveiller en temps réel la fréquence cardiaque, la qualité du sommeil, ou encore le niveau d'activité physique, et de transmettre ces données aux professionnels de santé.
- Des dispositifs médicaux comme les pompes à insuline sont capables d'ajuster automatiquement les doses en fonction des besoins du patient, renforçant ainsi la personnalisation des soins[2].

### 2. Transport et mobilité

Le secteur du transport bénéficie largement des systèmes M2M/IoT :

- Les véhicules connectés interagissent avec les infrastructures routières (feux, capteurs, panneaux intelligents) pour optimiser les trajets et réduire les risques d'accidents.
- Les systèmes de gestion de flotte permettent un suivi en temps réel de la position des véhicules (camions, bus), facilitant la logistique et la maintenance prédictive[2].

### 3. Énergie et environnement

Ces technologies sont également mobilisées pour une gestion plus durable des ressources :

- Les compteurs intelligents mesurent la consommation d'électricité, de gaz ou d'eau, et envoient automatiquement les données aux fournisseurs pour une facturation précise et une gestion énergétique optimisée.
- Les systèmes d'irrigation intelligents adaptent l'arrosage en fonction des conditions météorologiques, contribuant à une meilleure gestion de l'eau dans l'agriculture[2].

### 4. Maisons connectées (Smart Homes)

Les solutions domestiques basées sur l'IoT offrent un confort accru et une meilleure sécurité:

- Les thermostats intelligents (comme Nest) ajustent automatiquement la température selon les habitudes des occupants.
- Les appareils électroménagers (réfrigérateurs, machines à laver, fours) peuvent être commandés à distance via des applications mobiles.
- Les systèmes de sécurité intelligents détectent les intrusions, alertent les occupants et peuvent se connecter à des caméras ou alarmes pour une réaction rapide[2].

## I.5 Technologies biométriques : Face ID, Voice ID et Finger ID

Les systèmes d'authentification biométrique sont devenus des composantes essentielles dans les dispositifs de sécurité modernes. Parmi les plus répandus figurent la reconnaissance faciale (Face ID) et la reconnaissance vocale (Voice ID), ainsi que l'identification par empreinte digitale (Fingerprint ID). Ces technologies permettant d'identifier ou de vérifier l'identité d'un utilisateur à partir de caractéristiques physiques uniques.

### I.5.1 Face ID : reconnaissance faciale 3D

Le Face ID est une technologie de reconnaissance faciale tridimensionnelle permettant d'authentifier l'identité d'un utilisateur. Elle est couramment utilisée sur les smartphones, en particulier les iPhones, pour déverrouiller l'appareil, autoriser des paiements sécurisés ou accéder à des données sensibles [7].

Fonctionnement :

Le processus d'identification par Face ID repose sur plusieurs étapes :

- Capture en 3D du visage : Un module spécifique (caméra TrueDepth) projette des milliers de points infrarouges invisibles sur le visage afin de générer une carte en relief précise.
- Analyse biométrique : Cette carte est ensuite comparée au modèle enregistré lors de la configuration initiale.
- Sécurité renforcée : Les données faciales sont chiffrées et stockées localement dans une zone sécurisée appelée Secure Enclave, garantissant que ces informations ne quittent jamais l'appareil [7].

Face ID allie ainsi précision, rapidité et confidentialité, ce qui en fait une solution fiable pour une authentification sans contact dans divers contextes technologiques [7].

### I.5.2 Voice ID : reconnaissance vocale biométrique

Le Voice ID est une technologie qui repose sur l'identification biométrique de la voix, en s'appuyant sur la signature vocale unique de chaque individu. Elle permet d'authentifier un utilisateur à distance en analysant les caractéristiques propres à son timbre vocal [8].

Fonctionnement :

Le processus de reconnaissance vocale comprend plusieurs phases :

- Enregistrement initial : L'utilisateur fournit un ou plusieurs échantillons vocaux lors de la configuration.
- Analyse de la voix : Le système extrait plusieurs paramètres biométriques tels que le timbre, l'intonation, le rythme, et les fréquences vocales.
- Comparaison dynamique : À chaque tentative d'accès, un nouvel échantillon vocal est comparé aux données enregistrées pour valider l'identité [8].

## I.5.3 Finger ID : reconnaissance l'empreinte

### I.5.3.1 Contrôle d'Accès par Empreinte Digitale

Le contrôle d'accès par empreinte digitale, également appelé authentification biométrique dactyloscopique, est une méthode d'identification ou de vérification de l'identité d'un utilisateur basée sur les caractéristiques uniques de ses empreintes digitales**.** Chaque empreinte est constituée de crêtes et de vallées spécifiques à chaque individu, formant une signature biométrique permanente. Cette technologie permet à un système informatique de reconnaître une personne de manière fiable et sécurisée, sans nécessiter l'usage de mots de passe ou de clés physiques [9].

### I.5.3.2 Fonctionnement du système

Le processus d'authentification par empreinte digitale repose sur trois étapes principales :

1. **Enregistrement de l'empreinte digitale**
   L'utilisateur enregistre son empreinte dans le système à l'aide d'un capteur biométrique. Celle-ci est ensuite numérisée**,** traitée et stockée sous forme de données cryptées dans une base de données sécurisée [9].
2. **Vérification de l'empreinte**
   Lorsqu'un individu souhaite accéder à un espace ou à un appareil, il place son doigt sur le capteur. Le système scanne l'empreinte et la compare aux empreintes préalablement enregistrées [9].
3. **Décision d'autorisation ou de refus d'accès**
   Si une correspondance est détectée, l'accès est autorisé (déverrouillage de porte, activation d'un terminal, etc.). En cas d'échec de reconnaissance, l'accès est refuse [9].

### I.5.3.3 Avantages de cette technologie

L'authentification par empreinte digitale présente de nombreux avantages, tant en termes de sécurité que d'ergonomie :

1. **Sécurité renforcée**
   Chaque empreinte digitale étant unique, le risque de contournement du système est fortement réduit, rendant cette méthode très fiable [9].

2. **Confort d'utilisation**
   L'utilisateur n'a plus besoin de mémoriser des mots de passe ou de transporter des clés physiques, ce qui simplifie l'accès [9].
3. **Accès personnalisé**
   Le système permet l'enregistrement de plusieurs profils d'utilisateurs, avec des droits d'accès différenciés selon les besoins [9].
4. **Traçabilité des accès**
   Chaque authentification est horodatée et enregistrée, ce qui permet de consulter l'historique des entrées et sorties [9].
5. **Intégration avec d'autres systèmes**
   Cette technologie peut être reliée à des dispositifs IoT tels que des caméras de surveillance, des systèmes d'alarme**,** ou des systèmes d'éclairage automatisés**,** renforçant la cohérence de l'environnement sécurisé [9].

## I.6 Introduction au GSM

Le GSM (Global System for Mobile Communications) est une norme de téléphonie mobile développée en Europe à la fin des années 1980. Il a été conçu pour succéder aux systèmes analogiques de première génération en introduisant une solution numérique, offrant ainsi une meilleure qualité de communication, une interopérabilité internationale et de nouveaux services tels que les SMS, la confidentialité des appels, ou encore l'authentification des abonnés.

Adopté à l'échelle mondiale, le GSM est devenu pendant plusieurs décennies la norme dominante des communications mobiles, avant l'apparition des technologies de troisième, quatrième et cinquième générations (3G, 4G, 5G). En Europe, il fonctionne principalement sur les bandes de fréquences 900 MHz et 1800 MHz, tandis qu'en Amérique du Nord, les bandes 850 MHz et 1900 MHz sont utilisées [10].

### I.6.1 Architecture du Réseau GSM

Le réseau GSM repose sur une architecture modulaire composée de quatre sous-systèmes principaux**,** chacun jouant un rôle bien défini dans l'établissement, la gestion et la supervision des communications mobiles [10].

1. **MS – Mobile Station (Station Mobile)**

La Station Mobile est l'équipement utilisé par l'abonné, c'est-à-dire le téléphone mobile**.** Elle comprend deux composants :

- **ME (Mobile Equipment)** : le terminal mobile lui-même.
- **SIM (Subscriber Identity Module)** : une carte à puce contenant les données d'identification de l'abonné, telles que l'IMSI et les clés de chiffrement [10].

**2. BSS – Base Station Subsystem (Sous-système de Stations de Base)**

Ce sous-système établit la liaison radio entre le mobile et le cœur du réseau GSM. Il est composé de :

- **BTS (Base Transceiver Station)** : antenne radio responsable de la transmission et de la réception des signaux vers/depuis les mobiles.
- **BSC (Base Station Controller)** : unité de contrôle qui gère plusieurs BTS, assure les transferts d'appel (handover), l'allocation des canaux radio, et la gestion des ressources radio [10].

**3. NSS – Network Switching Subsystem (Sous-système de Commutation Réseau)**

C'est le cœur du réseau GSM, chargé de la commutation des appels et de la gestion des abonnés. Il comprend :

- **MSC (Mobile Switching Center)** : gère l'établissement des appels et la mobilité des abonnés.
- **HLR (Home Location Register)** : base de données contenant les informations permanentes des abonnés (profil, services, localisation).
- **VLR (Visitor Location Register)** : base de données temporaire contenant les **données des abonnés présents** dans une zone géographique spécifique.
- **AUC (Authentication Center)** : centre chargé de **l'**authentification des abonnés et de la génération des clés de chiffrement.
- **EIR (Equipment Identity Register)** : base de données qui vérifie l'identité des équipements (téléphones autorisés ou interdits via des listes blanches ou noires) [10].

### 4. OSS – Operation and Support Subsystem (Sous-système d'Exploitation et de Support)

Ce sous-système est destiné à la gestion technique du réseau. Il assure :

- La **supervision en temps réel** du fonctionnement du réseau.
- La **maintenance préventive et corrective**.
- La **configuration des équipements** et l'**optimisation des performances** du réseau [10].

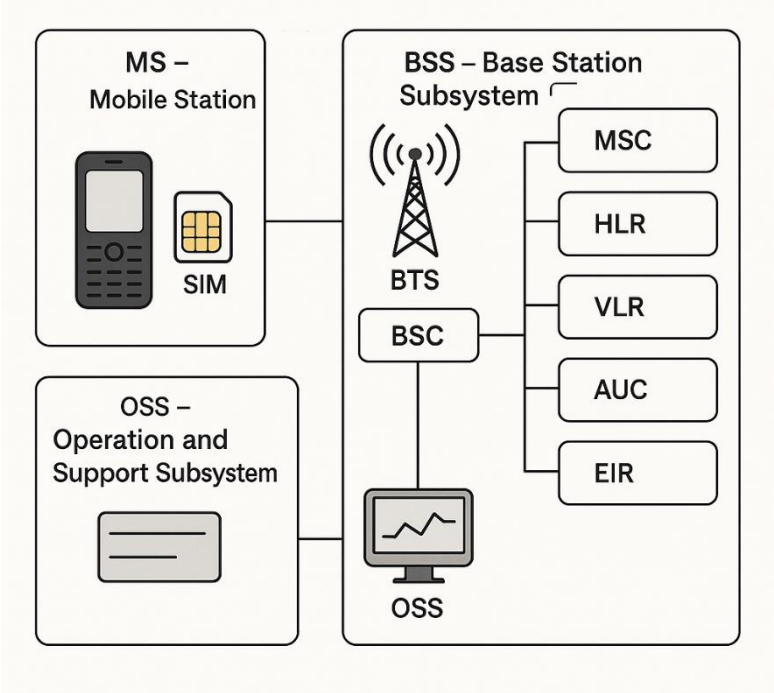



Figure 6 : Architecture du réseau GSM.

## I.6.2 Fonctionnement du GSM

Le fonctionnement d'un réseau GSM suit plusieurs étapes clés, allant de l'allumage du téléphone à la fin de la communication :

### 1. Allumage et enregistrement

- Lors de l'allumage, le mobile recherche la cellule GSM la plus proche.
- Il s'enregistre en envoyant son **IMSI** via la SIM.
- Le **MSC** interroge le **HLR** et le **AUC** pour valider l'abonné et l'autoriser à accéder au réseau [10].

### 2. Établissement d'un appel

- L'appel peut être initié par l'abonné ou reçu depuis le réseau.
- Le **MSC** établit une connexion via le **BSC** et le **BTS** concernés.
- Des ressources radio sont allouées pour la communication [10].

### 3. Handover (Transfert d'appel)

- Si l'abonné se déplace pendant un appel, le réseau effectue un handover pour transférer la communication vers une nouvelle cellule sans interruption [10].

### 4. Fin de communication

- Une fois l'appel terminé, les ressources radio et de commutation sont libérées, permettant leur réutilisation pour d'autres abonnés [10].

## I.7 Introduction à la 2G

La deuxième génération **(2G)** des réseaux mobiles marque une étape importante dans l'évolution des télécommunications. Mise en œuvre au début des années 1990, elle succède à la **1G**, qui utilisait des transmissions analogiques, en introduisant pour la première fois une communication entièrement numérique. Cette évolution a permis d'améliorer significativement la qualité, la sécurité et les services offerts aux utilisateurs.

Le **GSM** est le standard dominant de cette génération. Il a été conçu pour assurer une interopérabilité internationale, tout en offrant une capacité accrue, une meilleure efficacité spectrale et des services enrichis. [11]

### I.7.1 Objectifs de la 2G

Les principales motivations ayant guidé le développement de la 2G sont les suivantes :

- **Amélioration de la qualité des appels vocaux**, grâce à l'utilisation de codecs numériques.
- **Sécurisation des communications**, via des mécanismes de chiffrement intégrés.

- **Introduction de nouveaux services**, tels que les **SMS** (*Short Message Service*).
- **Optimisation de l'utilisation du spectre radio**, permettant une meilleure efficacité du réseau. [11]

### I.7.2 Architecture de la 2G (basée sur le GSM)

L'architecture de la 2G repose sur le modèle du réseau GSM, structuré en quatre sous-systèmes principaux, chacun jouant un rôle spécifique dans le traitement des communications et la gestion des abonnés :

1. **Station Mobile (MS)** :
   Terminal utilisé par l'utilisateur, comprenant le téléphone (**ME**) et la carte SIM contenant les données d'abonnement.
2. **Sous-système de stations de base** :
   Assure la communication radio avec le mobile via :
   - **BTS** (*Base Transceiver Station*) : antenne radio locale.
   - **BSC** (*Base Station Controller*) : contrôle plusieurs BTS, gère les ressources radio et les handovers.
3. **Sous-système de commutation réseau** :
   Constitue le cœur du réseau, il gère la commutation des appels, l'authentification, et la mobilité des abonnés à travers :
   - **MSC**, **HLR**, **VLR**, **AUC**, et **EIR**.
4. **Sous-système d'exploitation et de support (OSS)** :
   Permet la gestion, la supervision et la maintenance de l'ensemble du réseau GSM. [11]

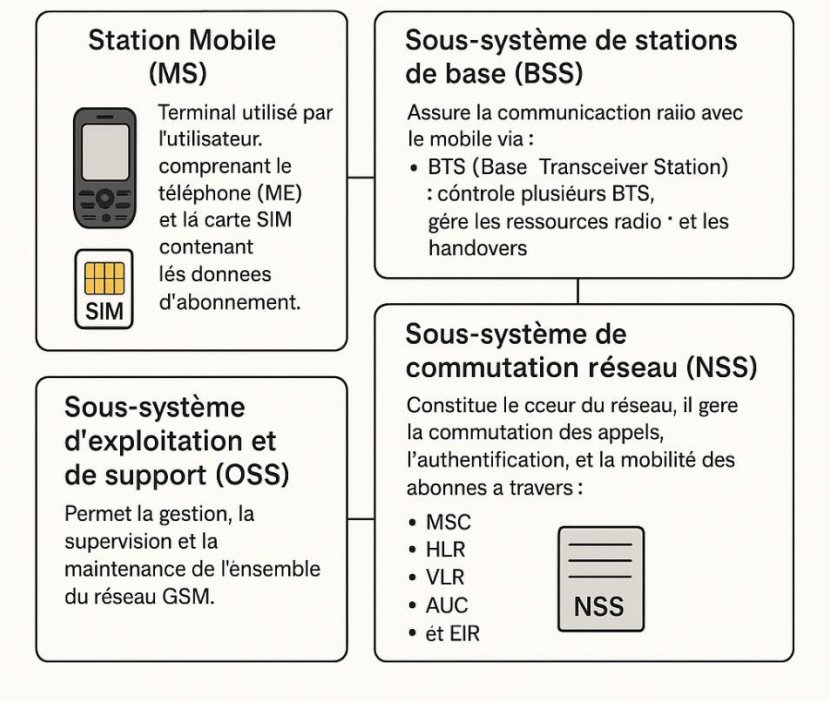



Figure 7 : Architecture de la 2G

### I.7.3 Fonctionnement de la 2G (GSM)

1. **Connexion au réseau**

Lorsqu'un téléphone est allumé, il recherche automatiquement la **BTS** la plus proche et tente de s'y connecter. Le **MSC** vérifie ensuite l'identité de l'abonné à l'aide des informations contenues dans la **SIM**, via l'interrogation du **AUC**.

2. **Établissement d'un appel**

Quand un appel est initié ou reçu, le **MSC** établit une liaison entre les correspondants. Si l'utilisateur est en déplacement, un **handover** est effectué pour assurer la continuité de la communication d'une cellule à une autre.

3. **Transmission de SMS**

Les messages courts (SMS) transitent par le **SMSC** (*Short Message Service Center*), qui assure leur transmission et, si nécessaire, leur stockage temporaire.

4. **Transmission de données (GPRS – 2.5G)**

L'évolution vers la **2.5G** avec le **GPRS** (*General Packet Radio Service*) permet l'accès à Internet à un débit modéré (jusqu'à **114 kbps**) en introduisant un **mode de transmission par paquets**, adapté aux données.

5. **Sécurité**

La 2G introduit plusieurs mécanismes de **protection des communications** :

- **Chiffrement** des échanges via l'algorithme **A5**.
- **Authentification** de l'abonné par une **clé secrète (Ki)** stockée dans la **SIM**.
- Utilisation de l'**IMSI** (identité internationale d'abonné mobile) et de son alias temporaire (**TMSI**) pour préserver la confidentialité. [11]

| **Caractéristiques** | **Détail** |
|---|---|
| Technologie principale | GSM |
| Bande de fréquences | 850 / 900 / 1800 / 1900 MHz |
| Accès multiple | TDMA (8 utilisateurs par canal radio) |
| Modulation | GMSK (Gaussian Minimum Shift Keying) |
| Débit | Jusqu'à 14.4 kbps (GSM) / 40-50 kbps (GPRS/EDGE) |
| Services offerts | Appels, SMS, services de base de données |

Tableau 1 : Caractéristiques techniques de la 2G [11].

## I.8 Conclusion

À travers ce chapitre, nous avons mieux compris l'importance des technologies M2M et IoT dans le monde moderne.

Leur capacité à connecter des objets physiques et à automatiser les échanges d'informations ouvre la voie à de nombreuses innovations, notamment dans le domaine de la sécurité des maisons intelligentes.

L'analyse des architectures, des protocoles de communication et des cas d'usage a permis de mieux cerner les enjeux techniques liés à l'implémentation de ces technologies.

Ces notions constituent une base théorique essentielle pour aborder la partie suivante, qui sera consacrée à la présentation des composants matériels de notre système de sécurité biométrique.

# CHAPITRE II :

# Présentation du Projet

# CHAPITRE II: Présentation du projet

## II.1 Introduction

Dans ce chapitre nous présentons les outils matériels et environnements logiciels utilisés pour développer notre système et ainsi que les différentes plateformes d'exécution de ses différentes parties.

## II.2 Présentation du cahier des charges

Notre système est basé sur une carte Arduino connectée à certains capteurs et actionneurs.

Pour la réalisation de notre système nous avons besoin des éléments suivants :

1. Arduino uno
2. Servo motor
3. PIR Sensor
4. LCD`
5. Buzzer
6. FingerPrint Sensor
7. Clavier Matriciel 4*4
8. Gsm SIM800L

## II.3 Les outils matériels

### II.3.1 La carte Arduino

#### II.3.1.1 Historique

L'Arduino est à l'origine un projet d'étudiants de l'école de Design d'Interaction d'Ivrea en Italie. Au début des années 2000, les outils de conception de projets dans le domaine du design d'interaction étaient onéreux, proches d'une centaine d'euros. Ces outils étaient pour la plupart conçus pour le domaine de l'ingénierie et de la robotique. Maîtriser et utiliser ces composants demandait beaucoup de temps et d'apprentissage et ralentissait fortement le processus de création pour ces jeunes étudiants.

Leur vient alors à l'idée de créer une plateforme plus abordable et plus simple à utiliser, reposant sur l'environnement de développement Processing mis au point en 2001 par des étudiants du MIT. C'est donc en 2003 que, pour un projet de fin d'études, fut conçue la carte Wiring, ancêtre de l'Arduino. Visant à rendre la plateforme toujours moins chère et plus accessible, une équipe d'étudiants et de professeurs finirent par concevoir la toute première Arduino en 2005. Entièrement open source, l'Arduino présentait l'avantage d'être multiplateforme et d'être en perpétuelle optimisation par la communauté d'utilisateurs. [12]

### II.3.1.2 Présentation générale

Les cartes Arduino sont conçues pour réaliser des prototypes et des maquettes de cartes électroniques pour l'informatique embarquée. Ces cartes permettent un accès simple et peu couteux à l'informatique embarquée. De plus, elles sont entièrement libres de droit, autant sur l'aspect du code source (Open Source) que sur l'aspect matériel (Open Hardware). Ainsi, il est possible de refaire sa propre carte Arduino dans le but de l'améliorer ou d'enlever des fonctionnalités inutiles au projet.

Le langage Arduino se distingue des langages utilisés dans l'industrie de l'informatique embarquée de par sa simplicité. En effet, beaucoup de librairies et de fonctionnalités de base occulte certains aspects de la programmation de logiciel embarquée afin de gagner en simplicité. Cela en fait un langage parfait pour réaliser des prototypes ou des petites applications dans le cadre de hobby. Le système Arduino permet de :

– Contrôler les appareils domestiques

– Fabriquer votre propre robot

– Faire un jeu de lumières

– Communiquer avec l'ordinateur

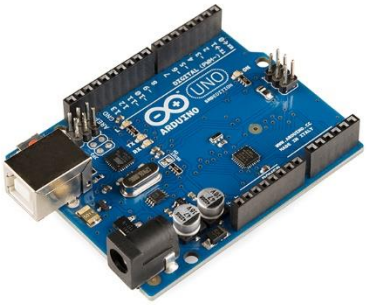
– Télécommander un appareil mobile (modélisme) [12]

### II.3.1.3 Types de carte Arduino

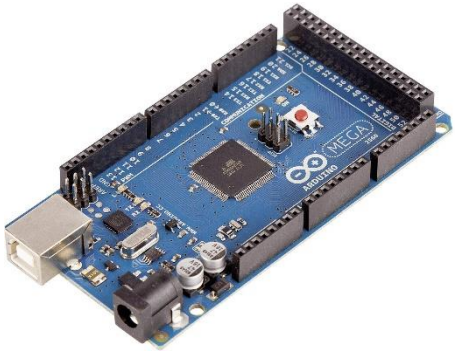
Il existe plusieurs types de carte Arduino, nous citons :

- Arduino Uno
- Arduino Méga

- Arduino Nano
- LilyPad Arduino
- Arduino Leonardo
- RedBoard [12]

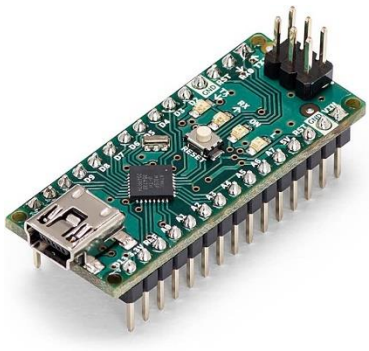


a- Arduino Uno



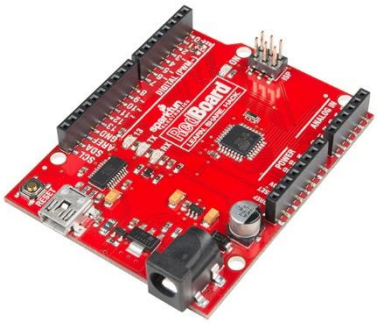
b- Arduino Mega

c- Arduino LilyPad



d- Arduino Nano

e- Arduino Leonardo



f- Red board

Figure 8 : Différents types d'Arduino [12].

Dans notre projet, nous avons utilisé la carte Arduino Uno.

### II.3.1.4. La carte Arduino Uno

#### II.3.1.4.1 Présentation

La carte Arduino Uno est le produit populaire parmi les cartes Arduino. Parfaite pour débuter la programmation Arduino, elle est constituée de tous les éléments de base pour construire des objets d'une complexité relativement faible. La carte Arduino Uno, comme son nom l'indique, a été la première à utiliser la version de programmation Arduino 1.0, et elle est devenue le symbole de l'univers Arduino.

La carte Arduino Uno est constituée de 14 broches d'entrées/sorties digitales, dont six sont utilisables en PWM, de 6 broches d'entrées analogiques, d'une connectique USB, d'une connectique d'alimentation, d'un port ICSP et d'un bouton RESET.[12]

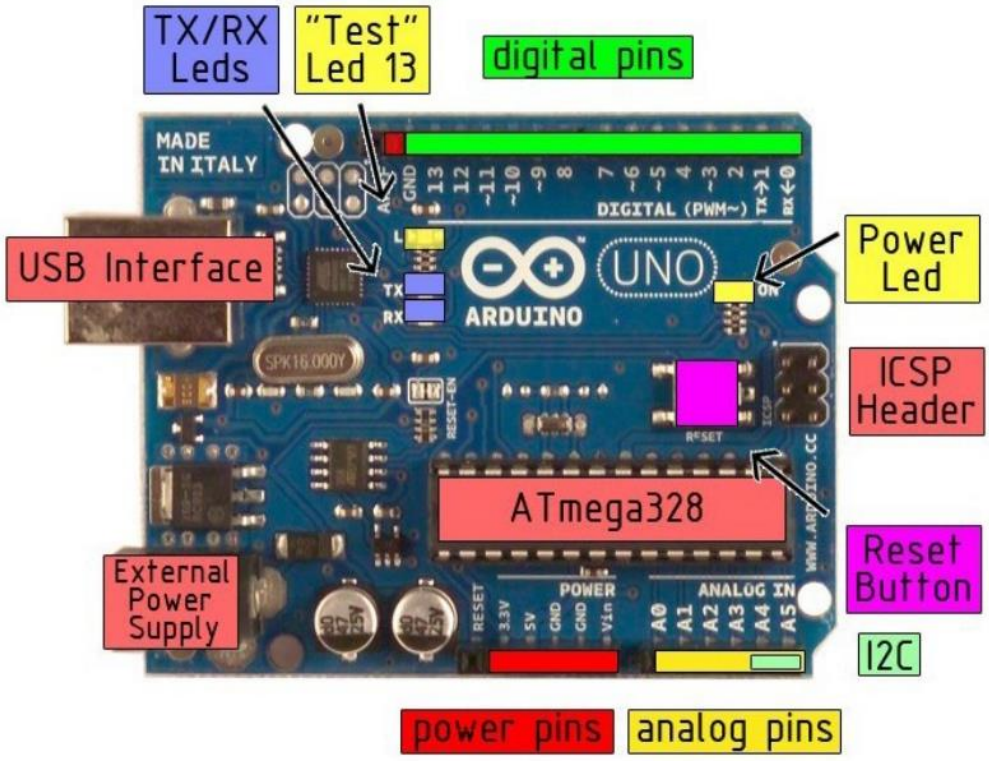



Figure 9 : Description des entrées/sorties de la carte Arduino Uno

L'alimentation de la carte Arduino Uno se fait normalement entre 7V et 12V de courant continu. Cependant, il est possible de faire fonctionner la carte Arduino Uno au maximum entre 6V et 20V. En deca de 6V, la carte n'est plus stable. Au-delà de 20V, le régulateur de tension sur chauffe, et peut endommager la carte.

L'alimentation de la carte peut se faire à travers le port USB lorsqu'il est branché sur l'ordinateur, ou via la connectique d'alimentation avec le port jack ou l'entrée d'alimentation. L'alimentation est sélectionnée de manière automatique par la carte Arduino. La source d'alimentation fournissant le meilleur voltage sera sélectionnée comme source d'alimentation par la carte.

En utilisant la connectique d'alimentation, une batterie ou un chargeur spécifique délivrant un courant continu de 9V convient parfaitement pour alimenter d'autres éléments.

L'entrée d'alimentation (VIN) permet d'utiliser une broche afin d'alimenter votre carte Arduino en électricité. Il est conseillé d'utiliser une alimentation entre 7V et 12V de courant continu pour ne pas endommager la carte.

La broche 5V est une connexion de sortie permettant de récupérer un courant généré par le régulateur de la carte. La broche 3.3V permet aussi de récupérer un courant mais de 3.3V et de 50 mA au maximum. Les prises de terre ou GND permettent de fermer le circuit.

Les broches d'entrées et sorties pour la carte Arduino Uno peuvent être décrites en deux parties. Les 14 broches d'entrées et sorties digitales sont utilisables comme leur nom l'indique en entrée ou en sortie en utilisant les fonctions pinMode, DigitalRead/ ou DigitalWrite. Chaque broche opère à 5V et peut fournir ou recevoir au maximum 40mA. De plus, chaque broche dispose d'une résistance interne de 20 à 50 kΩ, non connectée par défaut.

La carte Arduino UNO possède également six broches d'entrées analogiques étiquetées d'A0 à A5. Elles mesurent l'entrée de courant sur 5V sur une résolution de 10 bits, soit sur une échelle de 0 à 1023.Sur les broches A4, appelée aussi broche SDA, et A5, appelée broche SCL, il est possible de gérer la communication I2C.

D'un point de vue plus technique, cette carte se base sur le processeur ATmega328, un puissant microcontrôleur disposant d'une mémoire flash qui donne des performances très élevées tout en ayant une basse consommation. Il dispose d'une mémoire de 32 Ko, et de 2 Ko de SRAM. Il possède également une mémoire de 2 Ko d'EEPROM, programmable en utilisant la librairie EEPROM. [12]

#### II.3.1.4.2 Les Caractéristiques techniques :

| **Composant** | **Caractéristiques** |
|---|---|
| Microcontrôleur | ATmega328 |
| Tension de fonctionnement | 5v |
| Tension d'Input | 7-12v |
| Tension d'Input (limites) | 6-20v |
| Pins I /O digitales | 14 (dont 6 fournissent une sortie PWM) |
| Pinces d'E / S numériques PWM | 6 |
| Pins Input Analogiques | 6 |
| Courant DC par pin I/O | 20 Ma |
| Courant DC pour la broche 3.3V | 50 Ma |
| Mémoire flash | 32 Ko (ATmega328P) ; 0,5 Ko utilisé par bootloader |
| SRAM | 2KB(ATmega328) |
| EEPROM | 1 KB (ATmega328P) |
| Vitesse de l'horloge | 16 MHz |
| LED_BUILTIN | 13 |
| Longueur | 68.6 mm |
| Largeur | 53.4 mm |
| Poids | 25 g |

Tableau 2 : Les caractéristiques de l'Arduino Uno [12].

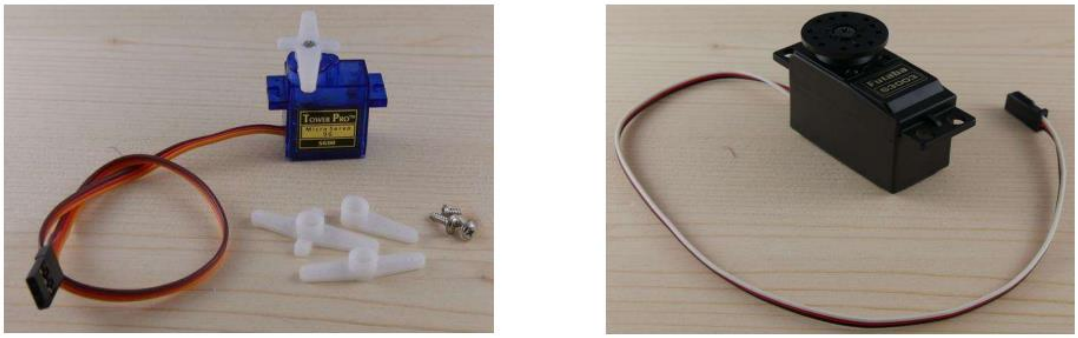
## II.3.2 Servo Moteur

### II.3.2.1 Définition

Un servo-moteur est un type de moteur électrique. C'est un dispositif typiquement utilisé en modélisme pour, par exemple, contrôler la direction d'une voiture télécommandée. Sur un servo-moteur, l'angle de l'axe reste fixé dans une position et peut varier entre 0 et 180° en fonction du signal envoy. [13]

### II.3.2.2 Les types de servo-moteur

Il existe divers types de servomoteur, de taille, poids et couple (force) différents.la photographie ci-dessous présente un servomoteur très classique en modélisme : le futuba S3003. Un peu plus bas l'article, on utilisera un autre servomoteur, communément appelé "servomoteur 9 grammes", par souci de consommation électrique. [13]



**a-** Servomoteur "9 grammes" **b -** .Servomoteur Futuba S3003

Figure 10 : types de servomoteur [13].

### II.3.2.3 Composition d'un servo-moteur

Le servomoteur est composé de plusieurs éléments visibles et invisible :

- Un moteur à courant continu
- Des engrenages pour former un réducteur (en plastique on en métal)
- Un capteur de position de l'angle d'orientation de l'axe (un potentiomètre)
- Une carte électronique pour le contrôle de la position de l'axe et le pilotage du moteur à courant continu

- Les fils, qui sont au nombre de trois
- L'axe de rotation sur lequel est monté un accessoire en plastique ou en métal
- Le boitier que le protège. [13]

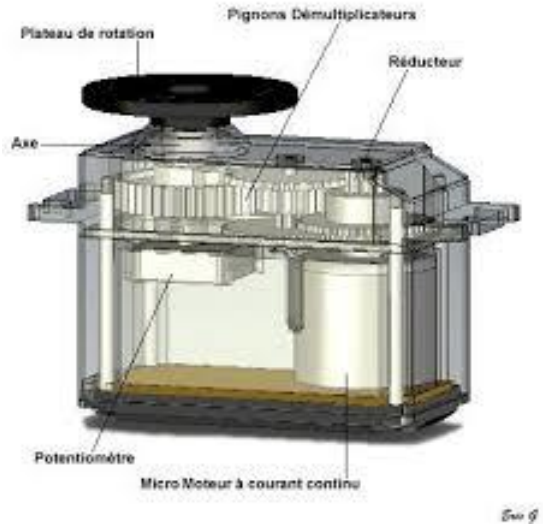



Figure 11 : Vue interne d'un servomoteur [13].

### II.3.2.4 Principe de fonctionnement d'un servo-moteur

La plupart des servomoteurs sont commandés par l'intermédiaire d'un câble électrique à trois fils qui permet d'alimenter le moteur et de lui transmettre des consignes de position sous forme d'un signal codé en largeur d'impulsion plus communément appelé PWM. Cela signifie que c'est la durée des impulsions qui détermine l'angle absolu de l'axe de sortie et donc la position du bras de commande du servomoteur. Le signal est répété périodiquement, en général toutes les 20 millisecondes, ce qui permet à l'électronique de contrôler et de corriger continuellement la position angulaire de l'axe de sortie, cette dernière étant mesurée par le potentiomètre. [13]

### II.3.3 Capteur de mouvement PIR

#### II.3.3.1 Présentation

Les capteurs PIR sont également connus sous le nom de capteurs infrarouges passifs. Ils sont conçus à partir d'une gamme de capteurs à semi-conducteurs fabriqués dans du matériel pyroélectrique générant une tension quand ils sont exposés à la chaleur. [14]

Figure 12 : Capteur de mouvement PIR [14].

#### II.3.3.2 Principe de fonctionnement

Le capteur PIR lui-même a deux fentes, chaque fente est faite d'un matériau spécial qui est sensible aux IR. L'objectif utilisé ici ne fait pas grand-chose et nous voyons donc que les deux fentes peuvent "voir" au-delà d'une certaine distance (essentiellement la sensibilité du capteur). Lorsque le capteur est inactif, les deux fentes détectent la même quantité d'IR, la quantité ambiante rayonnée par la pièce, les murs ou l'extérieur. Lorsqu'un corps chaud comme un humain ou un animal passe, il intercepte d'abord une moitié du capteur PIR, ce qui provoque un changement différentiel positif entre les deux moitiés. Lorsque le corps chaud quitte la zone de détection, l'inverse se produit, le capteur générant un changement différentiel négatif. Ces impulsions de changement sont ce qui est détecté [14].

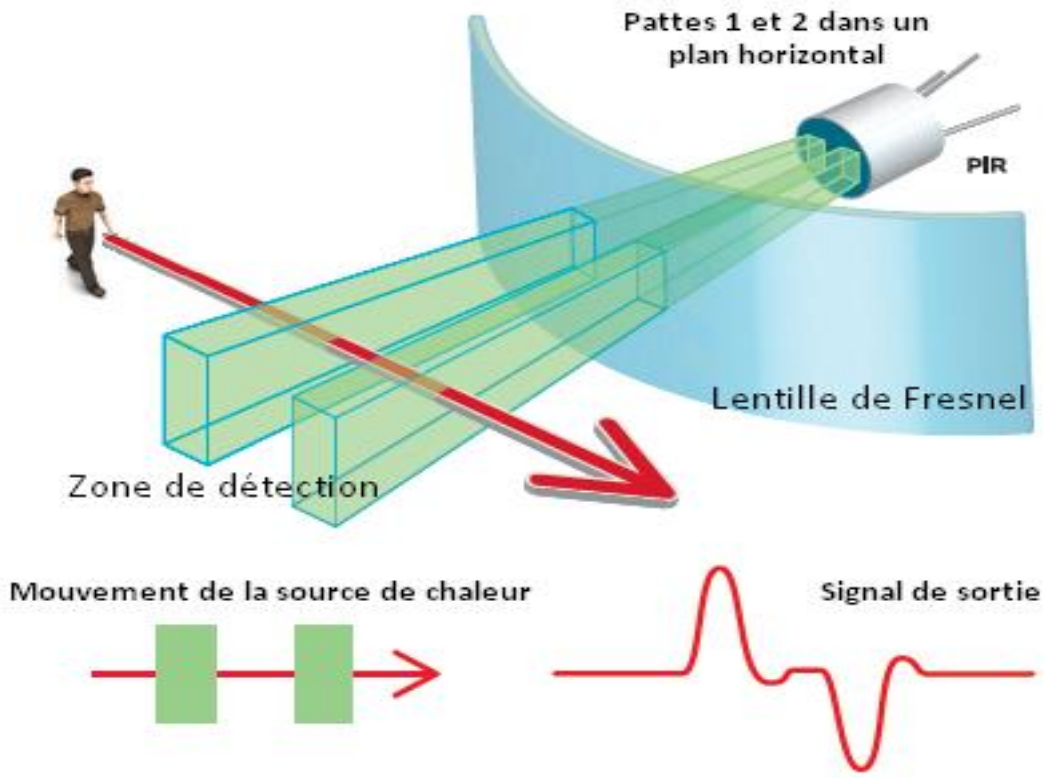



Figure 13 :Principe de détection du capteur PIR [14].

### II.3.3.3 Caractéristiques

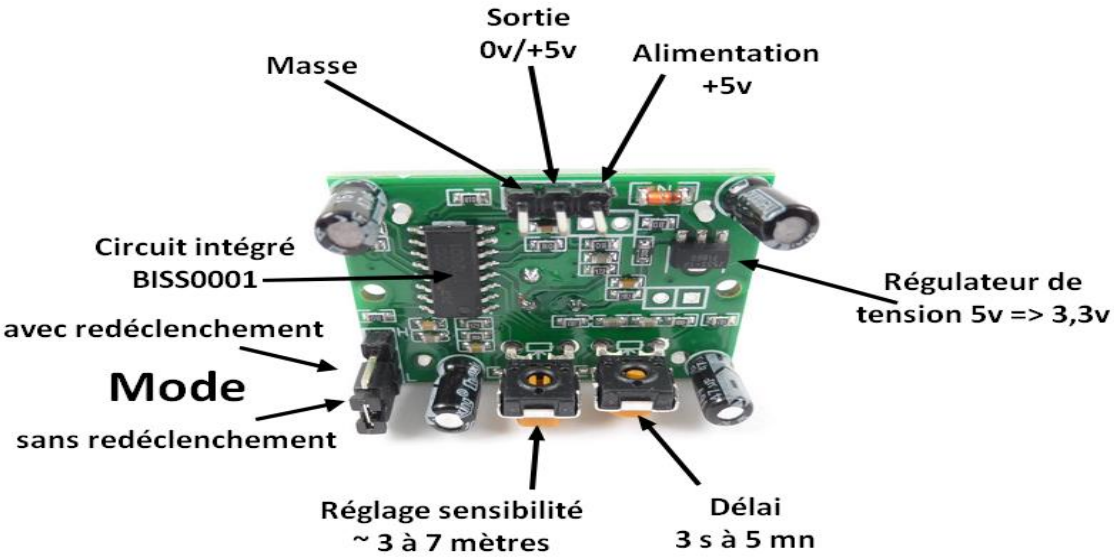



Figure 14 : Caractéristiques du capteur PIR [14].

- **GND :** Relier à la masse.
- **SORTIE :** Relier à une sortie digitale de l'Arduino.
- **VCC :** Relier à une alimentation 5V. [14]

Le capteur a également deux potentiomètres pour régler la sensibilité ainsi que le délai.

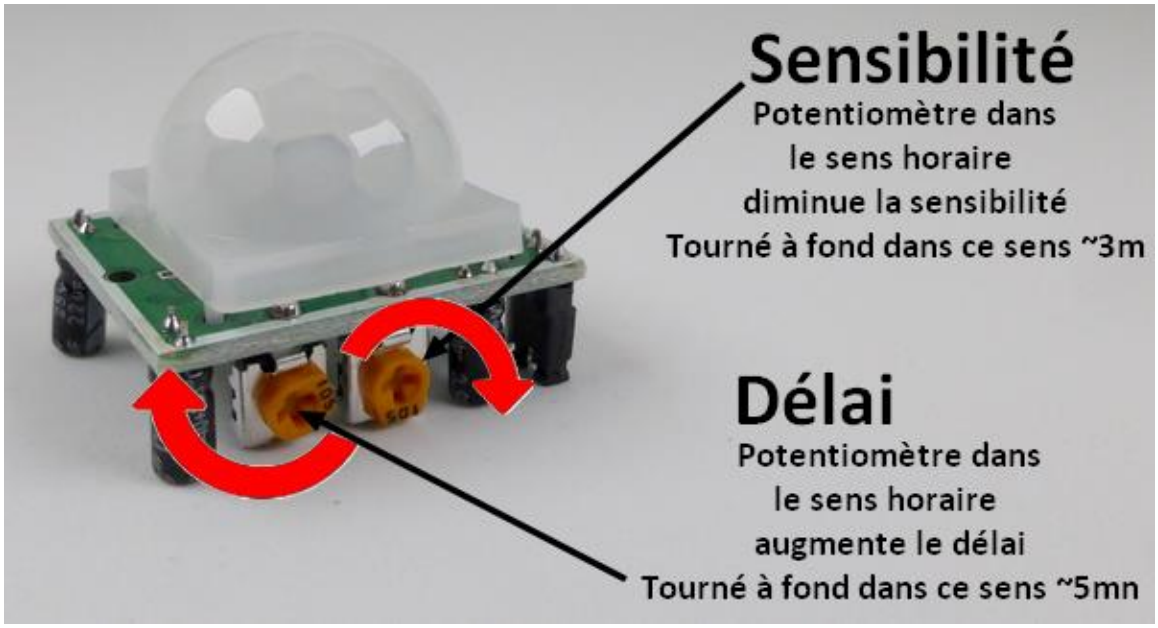



Figure 15 : Potentiomètre pour régler la sensibilité et le délai [14].

## II.3.4 Afficheur LCD

### II.3.4.1 Définition :

L'afficheur LCD est en particulier une interface visuelle entre un système (projet) et l'homme (utilisateur). C'est un dispositif électronique qui permet d'afficher des caractères, des nombres ou des symboles sur un écran. Son rôle est de transmettre les informations utiles d'un système à un utilisateur. Il affichera donc des données susceptibles d'être exploiter par l'utilisateur d'un système. Elles sont largement utilisées dans l'industrie électronique et dans de nombreux projets de bricolage en raison de leur faible consommation d'énergie, de leur faible encombrement et de leur coût abordable [15].

Figure 16 : Afficheur LCD [15].

### II.3.4.3 Caractéristiques de l'écran LCD :

L'afficheur LCD utilisé est composé de deux lignes de 16 caractères rétro-éclairé se raccordant via le bus I2C sur un microcontrôleur

Il existe plusieurs types d'afficheurs disponibles sur le marché, qui se distinguent les uns des autres par leurs dimensions (allant de 1 à 4 lignes et de 6 à 80 caractères), leurs caractéristiques techniques et leur tension de service. Certains modèles sont équipés d'un rétroéclairage, qui utilise des LED placées derrière l'écran du module [15].

- Les afficheurs LCD alphanumériques
- Les afficheurs LCD graphiques

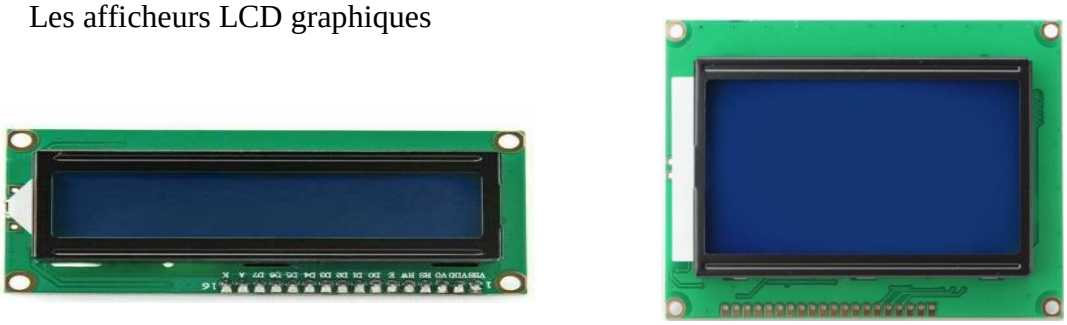


Figure 17 : types de d'afficheur LCD [15].

## II.3.5 Capteur d'empreintes AS608

### II.3.5.1 Présentation

Le module AS608 est un capteur d'empreintes digitales optique compact et efficace, utilisé pour la capture, la reconnaissance et la gestion d'empreintes digitales. Il est largement employé dans les systèmes de contrôle d'accès, les dispositifs biométriques et les projets basés sur Arduino et microcontrôleurs. Ce capteur peut scanner des empreintes et envoyer les données traitées à un microcontrôleur via une communication série. Toutes les empreintes enregistrées sont stockées dans le module, qui peut contenir jusqu'à 120 enregistrements d'empreintes individuels. Grâce à sa conception tout-en-un, l'AS608 facilite l'ajout de la détection et de la vérification des empreintes dans divers projets [16].

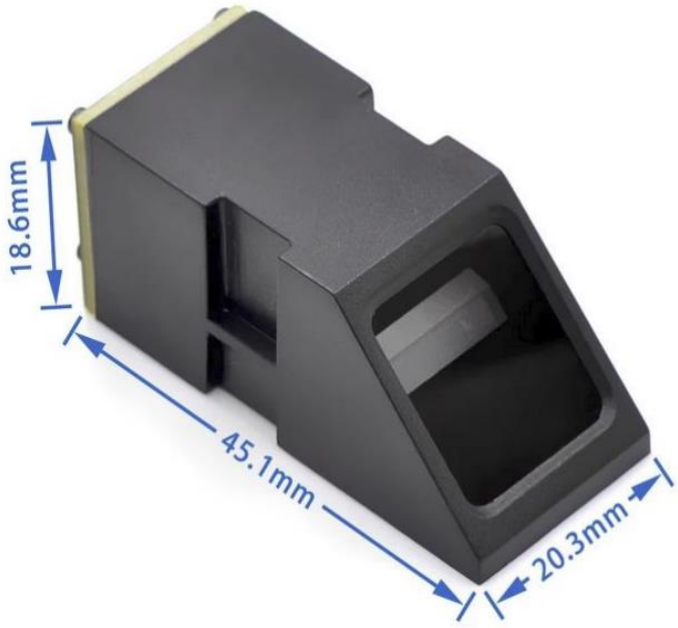



Figure 18 :capteur d'empreintes digitales AS608 [16].

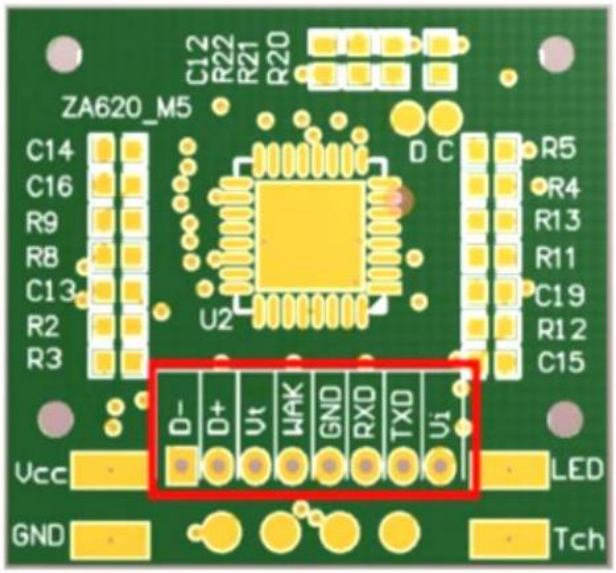



Figure 19 : AS608 Face composants [16].

### II.3.5.2 Les Caractéristiques techniques :

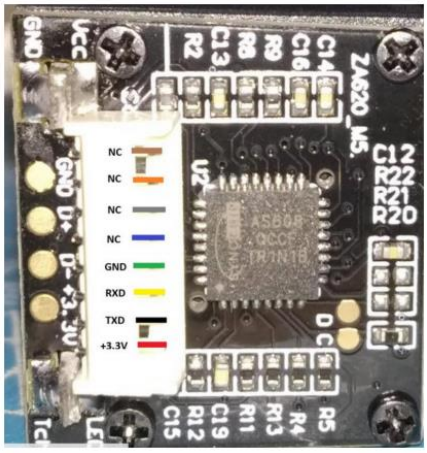



Figure 20 : Capteur AS608 – Vue arrière (brochage) [16].

| **Composant** | **Caractéristiques** |
|---|---|
| Nom | Module Lecteur d'Empreintes Digitales Optique AS608 |
| Tension de fonctionnement | (3.3~5)Vcc |
| Interface | Série TTL |
| Vitesse de transmission | (9600~57600) bauds (par défaut 57600) |
| Courant nominal | ~120 Ma |
| Temps de capture d'image | <1,0 seconde |
| Capacité de stockage | 162 modèles |
| Fichier modèle | 512 octets |
| Taux de fausse acceptation | <0,001% (niveau de sécurité 3) |
| Taux de faux rejet | <1,0% (niveau de sécurité 3) |
| Niveau de sécurité | De 1 à 5 (faible à élevé) |
| Température de fonctionnement | -20°C à +50°C |
| Fenêtre de detection | 16 mm × 18 mm |

Tableau 3 : Les caractéristiques de AS608 [16].

| **Pin Name** | **Pin Function** |
|---|---|
| V+ (Red) | Module power supply +3.3~5 V |
| TXD (Black) | Serial Data Output. TTL. |
| RXD (Yellow) | Serial Data Input. TTL. |
| GND (Green) | Ground |
| NC | No Connection |

Tableau 4 : Brochages du AS608 [16].

### II.3.5.3 Principe de fonctionnement

La peau de la main humaine présente des motifs uniques appelés crêtes de friction. Lorsqu'elle entre en contact avec une surface, ces crêtes établissent des points de contact directs, tandis que les vallées entre les crêtes restent légèrement éloignées de la surface.

Le capteur optique utilisé pour capturer ces motifs repose sur le principe de la Réflexion Totale Interne (TIR). Un prisme en verre dirige la lumière émise par une diode électroluminescente (LED) pour produire une réflexion interne complète en l'absence de tout contact. Lorsqu'un doigt est placé sur la surface, une onde évanescente est générée, influencée par la différence d'indice de réfraction entre la peau et l'air, entraînant un phénomène connu sous le nom de Réflexion Totale Interne Frustrée (FTIR). Cette modification est capturée par un capteur d'image et convertie en une image numérique de l'empreinte digitale.

Dans les capteurs capacitifs, qui offrent une précision supérieure, la lumière n'est pas utilisée. Une matrice de capteurs capacitifs détecte directement les variations dues aux crêtes et aux vallées, permettant ainsi de saisir des détails plus fins de l'empreinte [16].

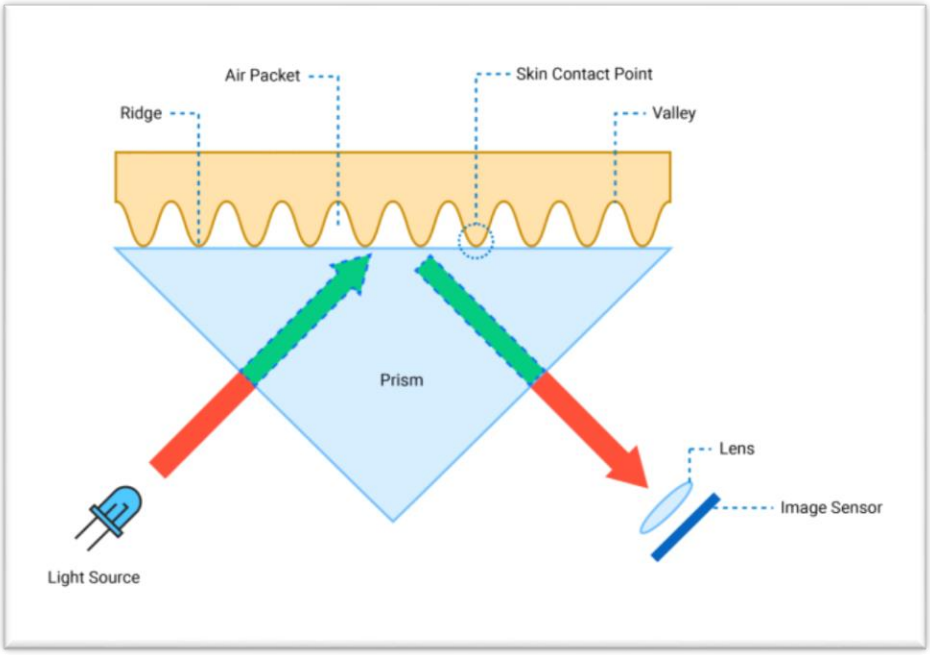



Figure 21 : Principe de Fonctionement [16].

## II.3.6 Buzzer

### II.3.6.1 Définition

Un buzzer est un dispositif électronique qui produit un son continu lorsqu'il est alimenté. Il est souvent utilisé dans les systèmes de signalisation pour indiquer un état ou une condition particulière, comme une alarme ou une notification. Les buzzers peuvent être activés de différentes manières, par exemple en utilisant un signal électrique ou en appuyant sur un bouton. Ils peuvent être contrôlés de manière précise en utilisant un microcontrôleur, ce qui permet de les intégrer dans une variété de projets électroniques, tels que les alarmes, les jouets et les appareils de mesure [17].

Figure 22 : Buzzer [17].

## II.3.7 GSM

### II.3.7.1 HISTORIQUE

Depuis l'année 1958 où le concept de téléphonie mobile est apparu. Les différents réseaux qui ont existé jusqu'au réseau actuel, le GSM, seront énumérés. Le premier réseau, le réseau A, était allemand et a fonctionné de manière manuelle, mais la technologie des téléphones mobiles n'était pas développée, ce qui a rendu les téléphones lourds et chers. Le deuxième réseau, le réseau B, a été utilisé en Allemagne et quelques pays limitrophes, mais il avait pour inconvénient de nécessiter la connaissance de l'emplacement de la personne pour la contacter. Le troisième réseau, le réseau C, est apparu en 1984 et a été le premier à utiliser les mêmes canaux de fréquences pour des cellules éloignées, mais chaque pays avait son propre standard. Ce réseau a servi à étendre les connaissances sur les réseaux cellulaires et a permis l'apparition de la carte SIM. Le réseau GSM est apparu en 1992 en Allemagne et est le premier système de radiotéléphonie entièrement numérique. Il fonctionne sur deux bandes, la bande GSM 900 et la bande DCS 1800, avec un total de 499 canaux alloués. Chaque canal peut gérer 8 utilisateurs grâce aux tranches de temps TDMA [18].

### II.3.7.2 Définition

Le GSM (Global System for Mobile Communication) est un réseau mobile numérique très répandu, surtout en Europe. Il utilise une forme de l'accès multiple par répartition dans le temps (AMRT) et constitue la technologie de téléphonie sans fil la plus utilisée parmi le TDMA, le GSM et le CDMA. Le GSM numérise et compresse les données, puis les transmet dans des créneaux temporels. Il fonctionne sur des bandes de fréquence de 900 MHz ou 1800 MHz. Ce système a évolué avec des technologies telles que le HSCSD, le GPRS, l'EDGE et l'UMTS, offrant ainsi une communication mobile fiable et standardisée à l'échelle mondiale. [10]

### II.3.7.3 Types de GSM

- GSM SIM800L
- GSM SIM7600
- GSM SIM868
- GSM M590E

- GSM A7

a- GSM SIM800L b- GSM SIM868 c- GSM A7

d- GSM SIM7600 e- GSM M590E

Figure 23 : Différents types de GSM [14].

Dans notre projet, nous avons utilisé GSM SIM800L

### II.3.7.4 GSM SIM800L

#### II.3.7.4.1 Présentation

Le module SIM800L GSM/GPRS est un modem GSM miniature. C'est un module puissant qui démarre automatiquement et recherche automatiquement le réseau. Ce module est idéal pour l'envoi de messages SMS ou de données sur un réseau mobile. Le contrôle s'effectue via lescommandes AT GSM standard à travers l'UART embarqué à partir du MCU connecté. Il permet d'émettre et recevoir des appels vocaux et d'envoyer et recevoir des messages SMS [14].


Figure 24 : GSM SIM800L [14].

#### II.3.7.4.2 Caractéristiques

Au cœur du module se trouve une puce cellulaire GSM SIM800L de SimCom avec une tension de fonctionnement de 3.4V à 4.4V. Le module prend en charge le débit en bauds de 1200bps à 115200bps avec détection automatique de transmission et a besoin d'une antenne externe pour se connecter au réseau. Le module est généralement livré avec une antenne hélicoïdale et se soude directement à la broche NET du PCB et dispose également d'un connecteur U.FL au cas où on voudrait éloigner l'antenne de la carte. Le GSM SIM800L est compatible avec les cartes SIM qui supporte la 2G [14].

Le module SIM800L a un total de 12 broches qui l'interfacent avec le monde extérieur. Les connexions sont les suivantes :


Figure 25 : GSM SIM800L Pinout [14].

| | |
|---|---|
| **NET** | **Broche pour souder l'antenne hélicoïdale** |
| **VCC** | **Alimentation de 3.7V à 4.4V** |
| **RST** | **Broche de réinitialisation matérielle** |
| **RXD / TXD** | **Communication série** |
| **GND** | **Doit être connecté au GND de l'Arduino** |
| **RING** | **Agit comme un indicateur de sonnerie** |
| **DTR** | **Active/désactive le mode veille** |
| **MIC+ / MIC-** | **Entrées microphone différentielles** |
| **SPK+ / SPK-** | **Interfaces de haut-parleurs différentiels** |

Tableau 5: Brochages du GSM SIM800 [14].

## II.4 Conclusion

Pour conclure, ce chapitre nous a permis d'explorer en profondeur l'ensemble des composants matériels nécessaires à la réalisation de notre système. Chacun de ces éléments, de la carte Arduino jusqu'au module GSM SIM800L, a été sélectionné en fonction de ses caractéristiques, de sa compatibilité et de sa pertinence par rapport aux objectifs du projet. Cette analyse nous permet de mieux appréhender les interactions entre les différents modules et de préparer efficacement la phase suivante, qui sera dédiée à l'implémentation et à l'intégration logicielle de notre solution.

# CHAPITRE III :

## Réalisation et Implémentation du Système de Sécurité Biométrique

## III.1 Introduction

Dans ce chapitre, nous abordons la phase de réalisation pratique de notre système de sécurité biométrique destiné à une maison intelligente. Après avoir présenté les fondements théoriques (IoT/M2M) et décrit les composants matériels, nous détaillerons le schéma de câblage des dispositifs, le code source embarqué sur la carte Arduino, la logique de fonctionnement du système ainsi que les résultats obtenus. Cette démarche nous permettra de valider l'intégration harmonieuse des différents modules et de mesurer les performances du système dans des conditions réelles.

## III.2 Schéma électrique

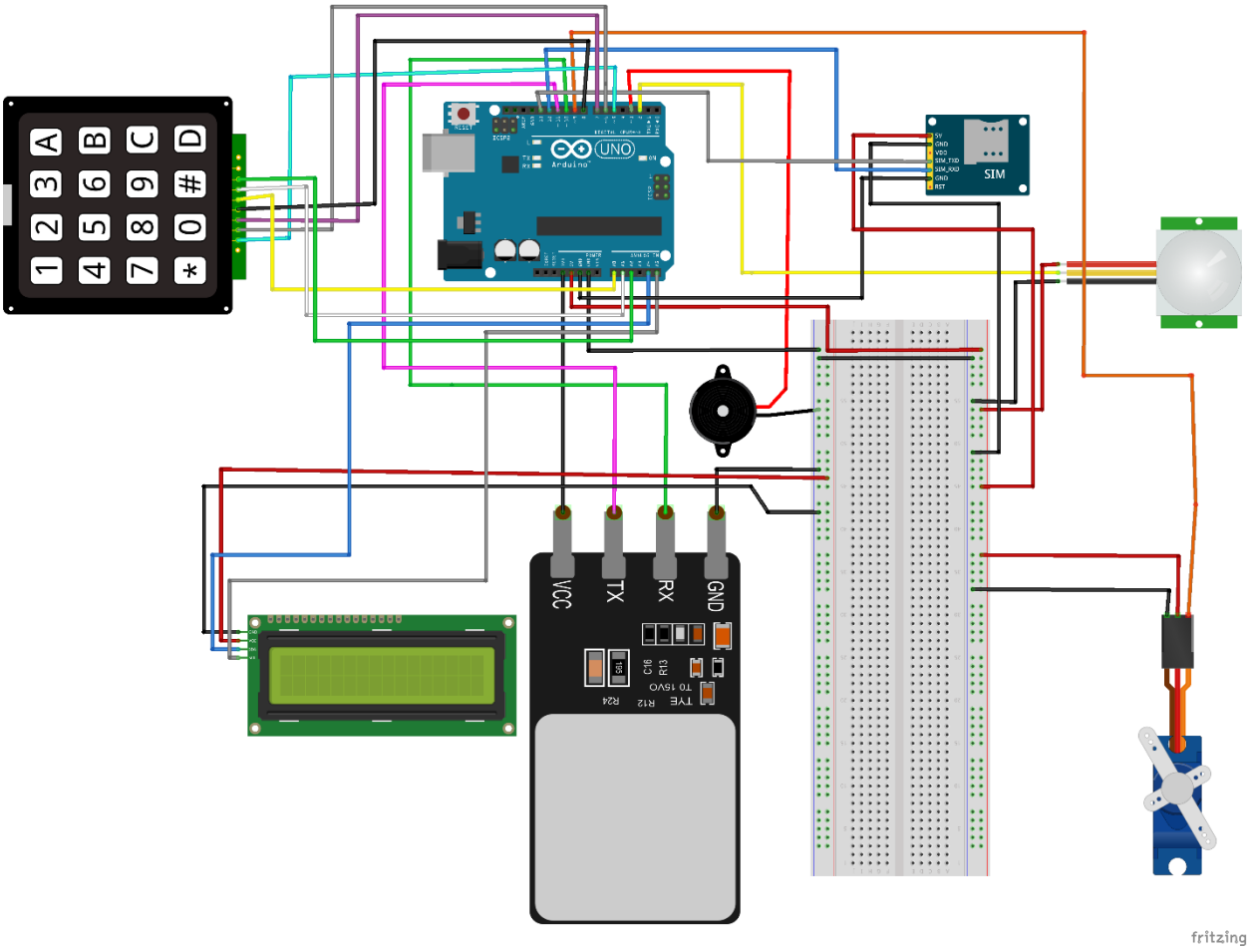



Figure 26 : Schéma électrique du prototype développé avec le logiciel Fritzing.

## III.3 Code Arduino

Afin de mettre en œuvre le système de sécurité biométrique proposé, nous avons développé un code embarqué basé sur la plateforme Arduino.

Ce code permet la gestion de l'ensemble des composants matériels du système, notamment le capteur d'empreintes digitales, le clavier matriciel, l'afficheur LCD, le servo-moteur, le capteur de mouvement PIR, le buzzer, ainsi que le module GSM SIM800L.

Il assure le fonctionnement séquentiel du système : activation par code PIN, identification biométrique, ouverture par servomoteur, notification par SMS, et déclenchement d'alerte en cas de détection de mouvement.

Le code suivant a été développé avec l'IDE Arduino, en utilisant plusieurs bibliothèques spécifiques (comme Adafruit_Fingerprint, Keypad, SoftwareSerial, Servo, etc.) pour une intégration optimale.

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Servo.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>

// Fingerprint sensor (D10 = RX, D11 = TX)
SoftwareSerial mySerial(10, 11);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

// GSM SIM800L (D12 = RX, D13 = TX)
SoftwareSerial Sim800l(12, 13);

// Servo motor
Servo myServo;
const int servoPin = 9;

// PIR Sensor & Buzzer
const int pirPin = 2;
const int buzzerPin = 3;

// LCD
LiquidCrystal_I2C lcd(0x27, 16, 2);

// Keypad
const byte ROWS = 4;
const byte COLS = 3;
char keys[ROWS][COLS] = {
  {'1', '2', '3'},
  {'4', '5', '6'},
  {'7', '8', '9'},
  {'*', '0', '#'}
};
byte rowPins[ROWS] = {5, 6, 7, 8};
byte colPins[COLS] = {A0, A1, A2};
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);

// Variables
bool systemActive = false;
String enteredPin = "";
const String correctPin = "369";

void setup() {
  Serial.begin(9600);
  mySerial.begin(57600);   // Fingerprint
  Sim800l.begin(9600);     // GSM Module

  Serial.println("Initializing...");
  myServo.attach(servoPin);
  myServo.write(0);

  lcd.init();
  lcd.backlight();
  lcd.print("Enter PIN:");

  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Fingerprint sensor detected!");
  } else {
    Serial.println("Fingerprint sensor NOT found. Check wiring.");
    while (1);
  }
```

```
  pinMode(pirPin, INPUT);
  pinMode(buzzerPin, OUTPUT);
}

void loop() {
  char key = keypad.getKey();

  if (key) {
    Serial.print("Key pressed: ");
    Serial.println(key);

    if (key == '#') {
      if (enteredPin == correctPin) {
        systemActive = !systemActive;
        lcd.clear();
        if (systemActive) {
          lcd.print("System ON");
          Serial.println("System Activated!");
        } else {
          lcd.print("System OFF");
          Serial.println("System Deactivated!");
        }
        delay(2000);
        lcd.clear();
        lcd.print("Enter PIN:");
      } else {
        lcd.clear();
        lcd.print("Wrong PIN!");
        Serial.println("Incorrect PIN!");
        delay(2000);
        lcd.clear();
        lcd.print("Enter PIN:");
      }
      enteredPin = "";
    } else if (key == '*') {
      enteredPin = "";
      lcd.clear();
      lcd.print("Enter PIN:");
    } else {
      if (enteredPin.length() < 4) {
        enteredPin += key;
        lcd.setCursor(enteredPin.length() - 1, 1);
        lcd.print('*');
      }
    }
  }

  if (systemActive) {
    checkFingerprint();
    checkPIR();
  }
}

void checkFingerprint() {
  int id = getFingerprintID();
  if (id >= 0) {
    String name = getNameFromID(id);
```

```
    Serial.print("Access granted to ID: ");
    Serial.println(name);

    lcd.clear();
    lcd.print("Welcome:");
    lcd.setCursor(0, 1);
    lcd.print(name);

    myServo.write(90);
    delay(7000);
    myServo.write(0);

    String message = "Access granted to: " + name;
    sendSMS(message);
  }
}

void checkPIR() {
  if (digitalRead(pirPin) == HIGH) {
    Serial.println("Motion detected! Possible intruder!");
    lcd.clear();
    lcd.print("Intruder Alert!");
    digitalWrite(buzzerPin, HIGH);

    // CALL USING SIM800L
    Sim800l.println("ATD+213540854106;"); // Replace with your number
    delay(1000);

    unsigned long startTime = millis();
    bool callActive = false;

    while (millis() - startTime < 30000) {
      if (Sim800l.available()) {
        String response = Sim800l.readString();
        response.trim();
        Serial.println("SIM800L Response: " + response);
        if (response.indexOf("CONNECT") != -1 || response.indexOf("OK") != -1) {
          callActive = true;
          break;
        }
      }
    }

    if (callActive) {
      Serial.println("Call connected. Holding for 10 seconds...");
      delay(10000);
      Sim800l.println("ATH");
      Serial.println("Call ended.");
    } else {
      Serial.println("No connection. Hanging up anyway...");
      Sim800l.println("ATH");
    }

    digitalWrite(buzzerPin, LOW);
    delay(1000);
  }
}

int getFingerprintID() {
  int p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;

```

```
  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) return -1;

  return finger.fingerID;
}

String getNameFromID(int id) {
  switch(id) {
    case 73: return "Bassem";
    default: return "ID " + String(id);
  }
}

void sendSMS(String message) {
  Sim800l.println("AT+CMGF=1"); // Set SMS to text mode
  delay(1000);
  Sim800l.println("AT+CMGS=\"+213540854106\"");
  delay(1000);
  Sim800l.print(message);
  delay(100);
  Sim800l.write(26); //
  delay(5000);
}
```

Ce code Arduino gère un système de sécurité biométrique combinant empreinte digitale, code PIN, détection de mouvement et communication GSM.

Après saisie du bon code PIN, le système s'active. Si une empreinte enregistrée est détectée, l'écran LCD affiche le nom de l'utilisateur, le servo s'ouvre 7 secondes, et un SMS est envoyé via la ligne Sim800l.println("AT+CMGS=\"+213540854106\"");.

En cas de mouvement détecté par le capteur PIR, une alerte sonore est déclenchée et un appel téléphonique est lancé automatiquement à l'aide de Sim800l.println("ATD+213540854106;");, puis raccroché avec Sim800l.println("ATH");.

Ce programme nécessite une carte SIM et une bonne connexion GSM pour l'envoi de SMS et d'appels.

## III.4 Schéma fonctionnel

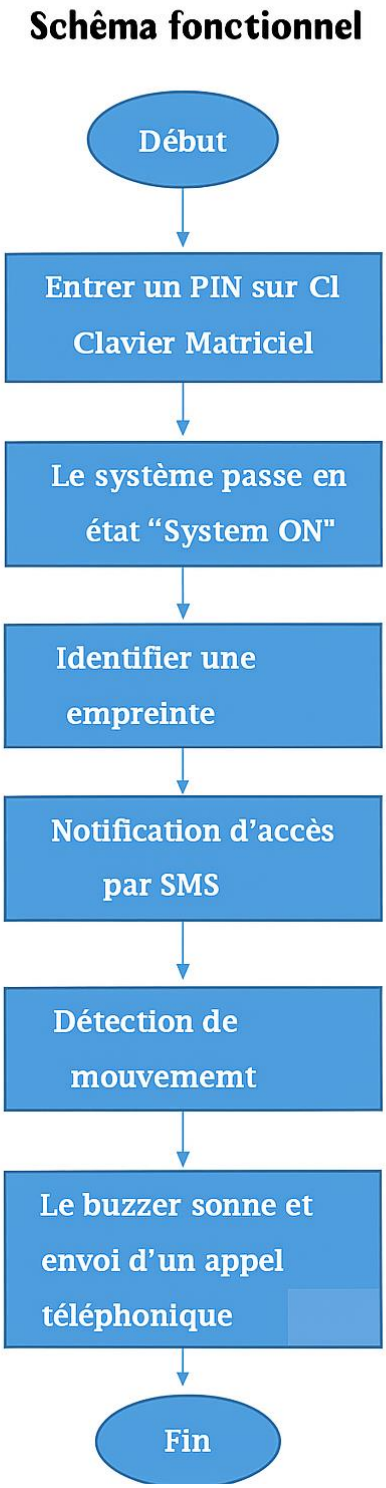



Figure 27 : Schéma fonctionnel du système de sécurité biométrique

## III.5 Méthodologie de mise en œuvre

Le fonctionnement de notre système de sécurité biométrique repose sur une séquence précise d'étapes orchestrées par la carte Arduino UNO :

1. **Activation du système**

   L'utilisateur saisit un code PIN sur le **clavier matriciel 4×4**. Si le code est correct, le système passe en mode actif.


Figure 28 : Entrée du code PIN via le clavier matriciel

Figure 29 : Clavier matriciel

2. **Confirmation visuelle**

   L'**écran LCD** affiche *« System ON »* pour indiquer que le système est prêt.

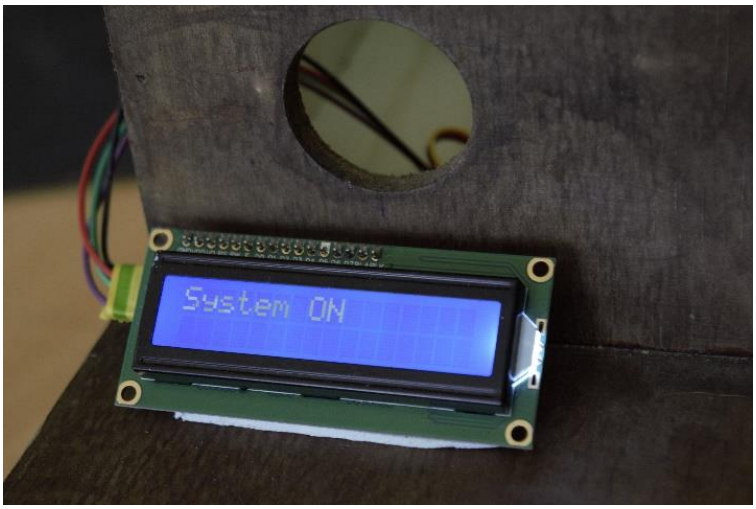



Figure 30 : Confirmation visuelle

3. **Identification biométrique**

   L'utilisateur place son doigt sur le capteur **AS608** ; en cas de correspondance, l'identité est validée. Après validation de l'empreinte, le **servo-moteur** s'active et libère l'accès.

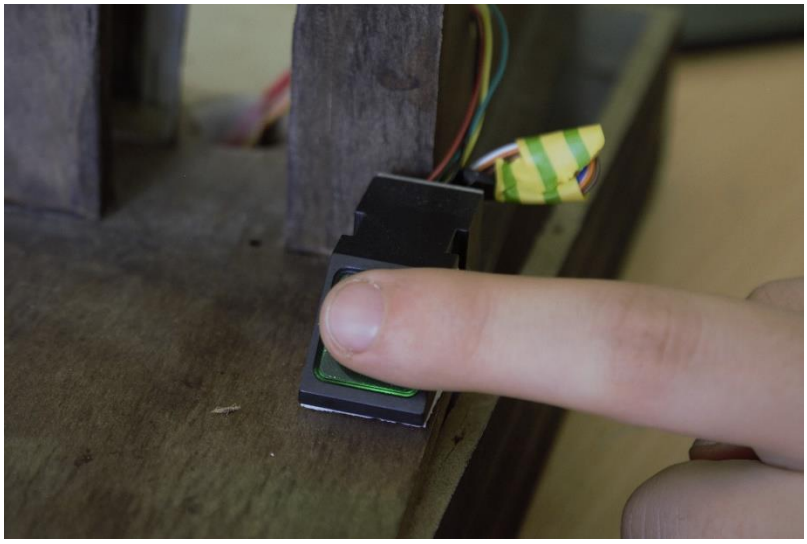


Figure 31 : Identification biométrique

4. **Affichage de l'identité**

   Le nom de l'utilisateur reconnu s'affiche sur le LCD pour confirmation.

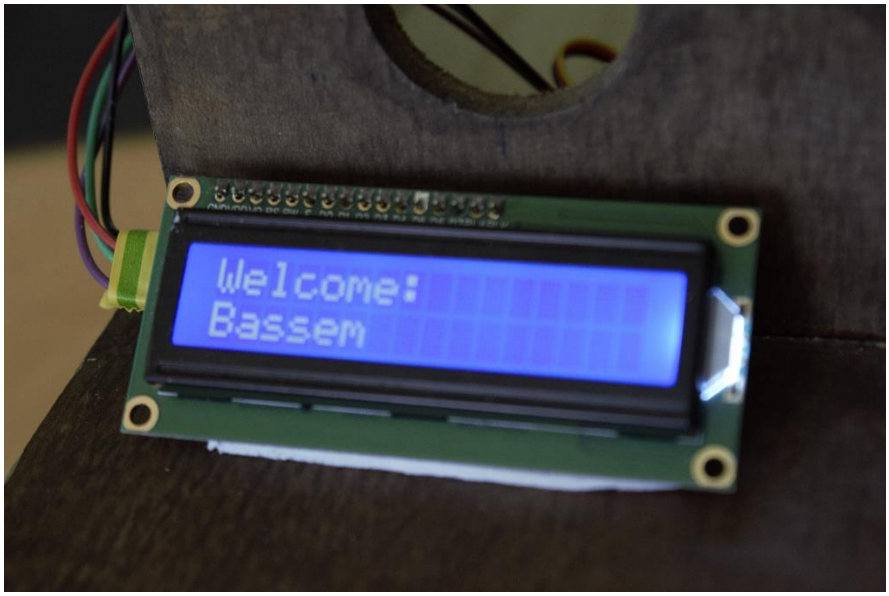



Figure 32 : Affichage de l'identité

5. **Notification par SMS**

   Un message contenant le nom de l'utilisateur est envoyé via le **module GSM SIM800L**.

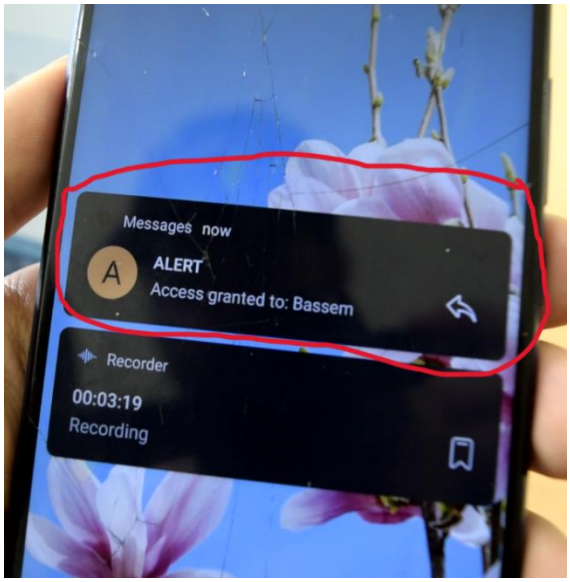
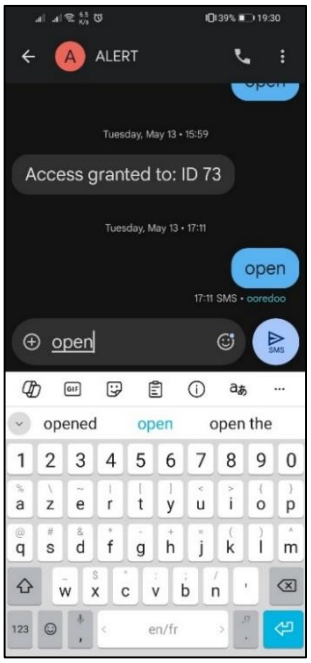



Figure 33 : Message SMS reçu par le propriétaire

6. **Déverrouillage à distance par SMS**

   Le propriétaire peut également envoyer un **SMS contenant un mot-clé ou un code d'autorisation** ; le module GSM analyse le message et, s'il est valide, déclenche l'ouverture du **servo-moteur** sans intervention locale.



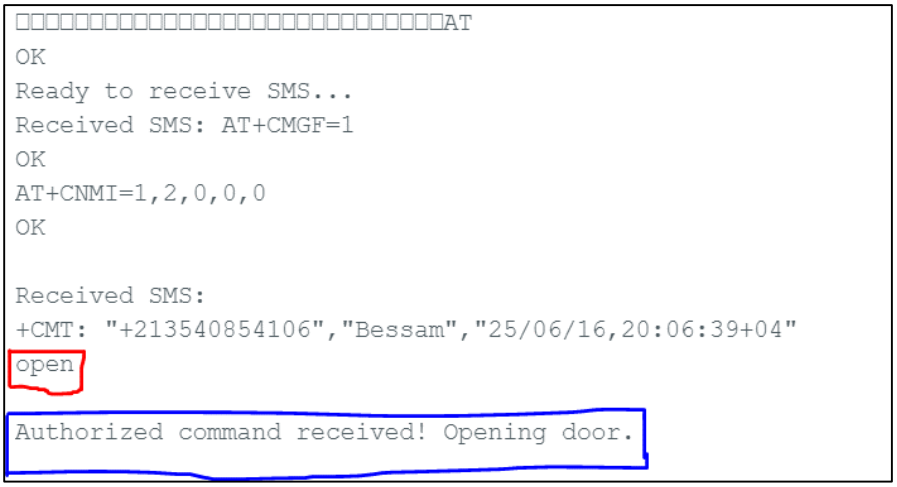




Figure 35 : Envoi de la commande SMS "open" Figure 34 : Interface de réception du SMS de déverrouillage

7. **Détection de mouvement & alarme**

   Si le **capteur PIR** détecte une présence non autorisée, le **buzzer** se déclenche et un **appel téléphonique** est lancé automatiquement pour alerter le propriétaire.

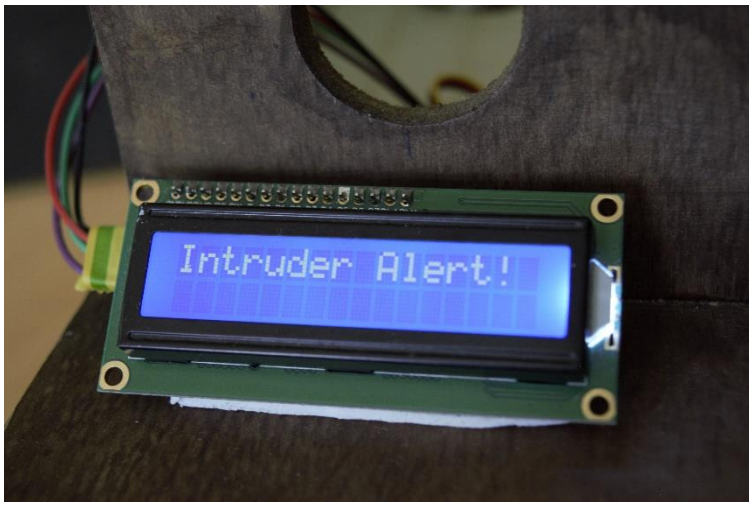



Figure 37 : Détection de mouvement par le capteur PIR

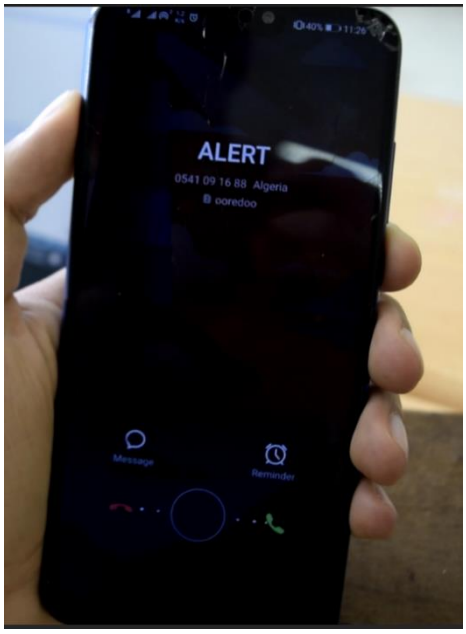



Figure 36 : Activation de l'alarme et appel automatique

## III.6 Discussion des résultats obtenus

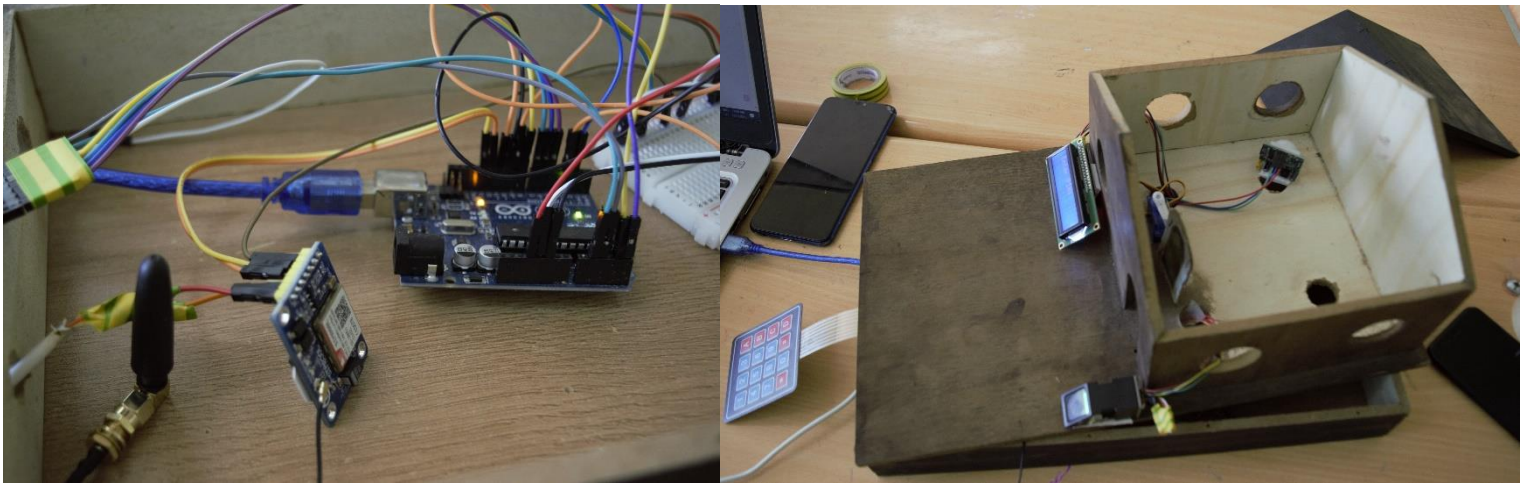


Figure 38 : Photo du prototype réalisé

Suite à l'implémentation complète de notre système de sécurité biométrique, plusieurs tests ont été réalisés dans un environnement contrôlé afin d'évaluer son efficacité et sa réactivité.

Les résultats montrent que le système fonctionne globalement de manière satisfaisante :

- L'identification via le capteur d'empreintes digitales AS608 est rapide et précise. L'utilisateur est reconnu instantanément si son empreinte est enregistrée.
- Le clavier matriciel permet d'activer le système de manière sécurisée grâce à un code PIN initial.
- L'écran LCD affiche correctement les messages d'état tels que *"System ON"* ainsi que le nom de l'utilisateur identifié.
- Le servo-moteur réagit sans délai après une identification réussie, permettant un accès rapide.
- Le module GSM SIM800L réussit à envoyer un SMS de notification contenant le nom de l'utilisateur identifié.
- En cas de détection de mouvement par le capteur PIR, le système déclenche correctement une alerte sonore via le buzzer, suivie d'un appel téléphonique vers le propriétaire.

Cependant, certaines limitations ont été rencontrées lors des tests :

- Incompatibilité avec certaines cartes SIM : dans certains cas, le module GSM n'arrivait pas à se connecter au réseau, ce qui empêche l'envoi de SMS ou d'appels.
- Retards dans la réception des SMS : il a été observé que les messages de notification n'arrivaient pas immédiatement, surtout lorsque la couverture réseau était faible.

Ces problèmes peuvent être liés à la qualité du signal GSM, à la compatibilité de certaines cartes SIM avec le module SIM800L, ou encore aux limites techniques du module lui-même.

Pour améliorer la fiabilité et les performances du système, plusieurs pistes d'évolution peuvent être envisagées :

- Ajouter une **vérification du niveau de signal GSM** avant chaque tentative d'envoi de SMS ou d'appel, afin d'éviter les échecs de transmission.

- Intégrer une **mémoire tampon locale** (EEPROM ou carte SD) pour stocker temporairement les événements en cas de perte de connexion réseau.
- Utiliser un **module GSM plus avancé** (comme SIM7600, compatible 4G) pour des communications plus rapides et stables.
- Remplacer ou compléter la carte Arduino par un **Raspberry Pi**, ce qui offrirait plus de puissance de traitement, la possibilité de gérer des bases de données locales, et d'exécuter des scripts plus complexes.
- Intégrer une **caméra de surveillance**, connectée au Raspberry Pi, permettant de capturer une image ou une courte vidéo de la personne identifiée ou de tout intrus détecté, et l'envoyer par mail ou l'enregistrer en local.

Ces améliorations rendraient le système plus robuste, plus intelligent et mieux adapté aux exigences actuelles en matière de sécurité des maisons intelligentes.

| **Critère** | **Fiche technique** | **Résultats expérimentaux** |
|---|---|---|
| Sensibilité du capteur PIR | 5m - 7m | 6m |
| Qualité GSM | Bonne | Bonne |
| Durée entre mouvement et appel | 2 s | 6 s |
| Durée d'exécution du programme | 20 ms | 30 ms |
| Temps de reconnaissance d'empreinte | 500 ms | 700 ms |
| Taux de reconnaissance | 98% | 95% |
| Temps de réception SMS | 4 s | 7s |
| Consommation approximative | 250 mA | 270 mA (mesurée) |
| Nombre de blocages du système | 0 (attendu) | 4 (observés) |

Tableau 6 : Comparatif entre les caractéristiques techniques et les résultats expérimentaux

### Comparaison et conclusion du tableau comparatif entre la fiche technique et les résultats expérimentaux

Ce tableau met en évidence les écarts entre les caractéristiques techniques attendues et les résultats observés lors des tests. Globalement, le système fonctionne conformément aux spécifications, notamment en ce qui concerne la détection, l'affichage et l'envoi de notifications. Cependant, certains écarts sont notables, comme le temps de réponse du système, les délais de réception des SMS et les blocages occasionnels.
Ces différences peuvent être attribuées à des facteurs tels que la qualité du réseau GSM, la complexité de l'environnement de test, ou encore les limitations matérielles des modules utilisés. Malgré cela, le système démontre une stabilité et une efficacité globales acceptables dans un contexte domestique. Des améliorations ciblées permettraient d'en optimiser davantage les performances.

## III.7 Conclusion

Ce chapitre nous a permis de concrétiser notre système de sécurité biométrique pour maison intelligente à travers l'intégration des différents composants matériels et le développement du programme embarqué. L'ensemble des tests réalisés a montré que le système fonctionne globalement comme prévu, avec une reconnaissance efficace des empreintes digitales, une réponse rapide des actionneurs, et une communication fonctionnelle via le module GSM. Malgré quelques limitations liées à la connectivité et au matériel, les résultats obtenus sont satisfaisants. Des pistes d'amélioration ont été proposées, notamment l'intégration d'un Raspberry Pi, l'ajout d'une caméra de surveillance, et l'optimisation des communications. Cette réalisation constitue une base solide pour le développement de systèmes de sécurité plus avancés et intelligents.

# Conclusion générale

À travers ce mémoire, nous avons exploré le développement d'un système de sécurité biométrique dédié aux Smart Homes, basé sur les technologies M2M et IoT.

Le premier chapitre nous a permis de comprendre les fondements des communications machine-to-machine et leur rôle crucial dans l'architecture de l'Internet des objets, qui constitue le socle de notre système intelligent.

Dans le deuxième chapitre, nous avons détaillé les composants matériels nécessaires, en analysant leurs caractéristiques techniques, leurs rôles respectifs, ainsi que leur pertinence dans le cadre du système envisagé.

Enfin, le troisième chapitre a été consacré à l'implémentation du système. Nous y avons présenté la méthodologie de travail, le câblage, le développement du code Arduino, et l'analyse des résultats. Cette phase pratique nous a permis de valider la faisabilité du projet et de réfléchir à des pistes d'amélioration futures.

En conclusion, ce projet constitue une contribution modeste mais concrète à l'intégration de solutions biométriques intelligentes dans les environnements domestiques. Il ouvre la voie à d'autres travaux plus avancés, exploitant des technologies émergentes pour renforcer la sécurité et le confort dans les maisons connectées.

## Références

[1] R. Haouari et I. Kermiche, *Déploiement des WSN par l'approche (BIM) dans les Smart-Building - IoT/M2M*, Mémoire de Master, 2023

[2] R. Maouche et O. Benchenouf, *Étude et conception d'un contrôle domotique d'une smart home*, Mémoire de Master, 2024.

[3] M. Chen, J. Wan, and F. Li, "Machine-to-Machine Communications: Architectures, Standards and Applications," *KSII Transactions on Internet and Information Systems*

[4] Cisco Systems, *L'Internet des Objets (IoT) – Un monde connecté*, Cisco

[5] R. Minerva, A. Biru, and D. Rotondi, "Towards a Definition of the Internet of Things (IoT)," *Procedia Computer Science*, 2018

[6] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, Apr. 2015

[7] Apple Inc., "À propos de Face ID avancé," *Support Apple*, Oct. 2023.

[8] A. H. Khan and P. S. Aithal, "Voice Biometric Systems for User Identification and Authentication – A Literature Review," *Int. J. Appl. Eng. Manag. Lett.*2022.

[9] A. K. Jain, L. Hong, and R. M. Bolle, "On-line Fingerprint Verification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302–314, Apr. 1997.

[10] M2M France, "Guide GSM – Comprendre le Réseau Global System for Mobile Communication," *M2M.fr*.

[11] I. ul Haq, Z. U. Rahman, S. Ali, and M. Faisal, "GSM Technology: Architecture, Security and Future Challenges," *Int. J. Sci. Eng. Adv. Technol. (IJSEAT)*, Jan. 2017.

[12] K. Hachemi, *Étude et réalisation d'un système d'alarme à base d'une carte Arduino*, Mémoire de Master, Département de Génie Électrique, Université Larbi Ben M'hidi - Oum El Bouaghi, Algérie, 2017.

[13] H. Hammioui and A. Frakcha, *Parking Intelligent*, Projet de fin d'études, Faculté des Sciences, Université Sidi Mohamed Ben Abdellah, Fès, Maroc, Jun. 2021.

[14] R. Char, *Gestion d'une maison intelligente*, Mémoire de Master, Département d'Électronique, Université Badji Mokhtar – Annaba, Algérie, 2021.

[15] "Afficheur LCD : comment l'exploiter ?," *Plaisir Arduino*

[16] AS608 Fingerprint Sensor Datasheet, Handson Technology

[17] "Fiche technique du buzzer : une explication détaillée," *MfgRobots*

[18] D. Andry, "Partie I : Historique des Réseaux mobiles.