



People's Democratic Republic of Algeria  
Ministry of Higher Education and Scientific Research  
MOHAMED KHIDER University - Biskra  
Faculty of Exact Sciences, Natural and Life Sciences  
Computer Science Department

Order N°: *GLSD\_Startup /M2/2025*

## Dissertation

Presented to obtain the academic Master's degree in Computer science

**Option:** Software Engineering and Distributed Systems (GLSD)

---

# Access control system based on Arduino Technology

---

**Presented by:**

Redjough Asma  
Zebila Djoumana Kaouther

**In Front of the Juries:**

Dr. Telli Abdelmoutia      President

Dr. Meklid Abdessalam      Examiner

Dr. Hamida Souraya      Supervisor

**Presented in 17 June 2025, University Year (2024 / 2025)**

## ***Acknowledgements***

*In the name of God, the Most Gracious, the Most Merciful.*

*First and foremost, we thank God Almighty for the countless blessings He has bestowed upon us,  
and for granting us the courage and patience to complete this work.*

*First, we thank ourselves for our efforts, patience, and ability to overcome the challenges  
we faced to achieve this project.*

*We would also like to extend our sincere thanks and appreciation to our supervisor,  
**Dr. Hamida Souraya,***

*for the time she allocated to us and for her assistance, as well as her patience and encouragement  
throughout our research.*

*We express our gratitude to all our professors in the Department of Computer Science at the  
Mohamed Khaidr University of Biskra, for their invaluable teaching, guidance,  
and knowledge they imparted to us during our years of study.*

*We also thank the jury members for their interest in our research and their agreement to discuss our  
dissertation.*

*Finally, we would like to thank everyone who contributed to the completion of this work:*

***Merabti Youcef, Labed Najib, Amdjed Sahra, Nassar Hamdan, and Redjouh Abdessatar.***

*Thank you all.*

## ***Dedication of Redjouh Asma***

*To the one who carried me in her heart long before I held a pen. To my beloved mother: the light of the path, the warmth of my days, and the calm of my life.*

*To my father, may he rest in peace... You left in body, but your heartbeat still echoes within mine. Your prayers live with me, your pride fuels me. You were the first to believe in me, and I will write with the ink of your love until my final line.*

*To my dearest siblings: Souhaib, Abde Sattar, Samah, and Nour. You were my shelter in life's storms, and my strength in every challenge. You are the faces I turn to for home, and the truest form of unconditional love.*

*To the sisters of my soul and joy: Rayan, Rawia, Nour houda, and Zaineb. You were the light in my nights of exhaustion, the laughter in moments of heaviness. With you, I learned that friendship is not just words, but a healing presence that heals the spirit.*

*To my late friend, Sara, the one I wanted to have beside me: between these pages and among the rows... May Allah have mercy on your soul. Though absent from sight, you remain forever in my heart. From these pages, a prayer is sent your way, and from every achievement, a share is yours.*

*To my companions in letters and the road: Samia, Djomana, Aya, and Donia. Thank you for walking beside me with wisdom, patience, and encouragement.*

*To everyone who contributed to this dissertation, whether through guidance, support, feedback, or simply believing in me, your role was vital, and your kindness will always be remembered.*

*This dissertation may have been written by my hand, but it was your hearts that filled the ink. To all of you, endless love and gratitude that time will never erase.*

## ***Dedication of Zebila Djoumana Kaouther***

*To the One who was with me in every moment, To the One I called upon and who answered, whom I trusted and who honored me To my Creator, to my Lord, All praise is due to You for every blessing I have received and completed. Praise be to God.*

*I also extend my gratitude to my teacher Hamida Souria for her support, no matter the circumstances.*

*To the one who taught me how to achieve what I want and to do what I desire, To the one who believed in me through everything, even in moments of despair... and said, "You can." To the one whose name I am carrying, and I hope to bring great pride to him, I dedicate this achievement to him.*

*To my dear mother, To the one who taught me that everything has a beginning, and that I have a Lord who knows my intentions, The one whose prayers accompanied me in every step and opened every path, The only one who felt weary from my fatigue and saddened by my sadness.*

*To Suham, my beloved my motivator and supporter, To my beautiful family my comfort and my strength in life, To the one who brightened my life with his arrival — a piece of my heart my brother Yazan, may God protect and care for you.*

*To my friends in all circumstances and days, To my classmates Asma, Aya, Donia, Dareen, Salsabeel, To my childhood friend Ronaq, and my dear Raneem, To everyone who has helped me one day, And to everyone who said, "You can't" you were a great motivation to keep going.*

*I hope my ambitions continue to rise, And today, I dedicate my graduation to all of you.*

## ***Abstract***

Access control systems are one of the most prominent security technologies used in smart institutions and homes, as they aim to restrict access to only authorized persons. The system also uses artificial intelligence techniques to enhance the process of verifying users' identities and resist attempts at forgery and imitation. A mobile phone application has been developed that allows the administrator to manage the process of registering authorized users, while a smart device is installed next to the door that enables the user to enter the secret code and his voice fingerprint by reading the unique generated sentence, to first verify that the spoken text matches the apparent sentence, then matches the voice. With the stored fingerprint. Upon successful verification, an encrypted password is sent via Bluetooth to the Arduino unit responsible for opening the door. The system was initially tested on a small group of users and the initial results showed good efficiency, indicating the efficiency of the system in real-world use conditions, noting some updates such as poor sentence pronunciation and loud noise. This system is characterized by a high level of security thanks to the double verification mechanism, in addition to ease of installation and low cost compared to other systems, which makes it a practical, flexible, and scalable solution to meet access control requirements within multiple environments.

**Keywords :** Access Control, Arduino, Voiceprint, Artificial Intelligence, Generative Artificial Intelligence.

## ملخص

تُعد أنظمة التحكم في الدخول من أبرز تقنيات الأمن المستخدمة في المؤسسات والمنازل الذكية، حيث تهدف إلى تقييد الوصول على الأشخاص المصرح لهم فقط. ومع التقدم التكنولوجي، زاد الاهتمام بابتكار حلول ذكية تعتمد على وسائل تحقق متعددة لتعزيز مستويات الأمان والمرونة. وفي هذا السياق، يهدف هذا المشروع إلى تصميم وتطوير نظام ذكي للتحكم في الدخول، يعتمد على وحدة اوردوينو ووسيلتي تحقق : رمز سري فريد (PIN) وبصمة صوتية. كما يستخدم النظام تقنيات الذكاء الاصطناعي لتعزيز عملية التحقق من هوية المستخدمين ومقاومة محاولات التزوير والتقليد. تم تطوير تطبيق هاتف محمول يتيح للمسؤول ادارة عملية تسجيل المستخدمين المخولين بالدخول، في حين يثبت جهاز ذكي بجانب الباب يمكن المستخدم من ادخال الرمز السري و بصمته الصوتية من خلال قراءة الجملة المولدة الفريدة، ليتم التحقق اولا من تطابق النص المنطوق مع الجملة الظاهرة، ثم مطابقة الصوت مع البصمة المخزن. وعند نجاح التحقق، ترسل كلمة سرية مشفرة عبر البلوتوث الى وحدة الوردوينو المسؤولة عن فتح الباب. تم اختبار النظام بشكل مبدئي على مجموعة صغيرة من المستخدمين، وأظهرت النتائج الاولوية كفاءة جيدة، مما يدل على كفاءة النظام في ظروف الاستخدام الواقعية مع الاشارة الى بعض التحديثات مثل عدم النطق الجيد للجملة والضوضاء العالية. يتميز هذا النظام بمستوى عال من الامان بفضل آلية التحقق المزدوج، الى جانب سهولة التثبيت وانخفاض التكلفة مقارنة بالانظمة الاخرى، مما يجعله حلاً عملياً مرناً وقابلاً للتطوير ليلبي متطلبات التحكم في الوصول ضمن بيئات متعددة.

الكلمة المفتاحية : التحكم في الوصول، اوردوينو، بصمة الصوت، الذكاء الاصطناعي، الذكاء الاصطناعي التوليدي .

## *Résumé*

Les systèmes de contrôle d'accès sont l'une des technologies de sécurité les plus utilisées dans les institutions et les maisons connectées, car ils visent à restreindre l'accès aux seules personnes autorisées. Avec les progrès technologiques, l'intérêt pour la création de solutions intelligentes s'appuie sur de multiples moyens de vérification pour améliorer la sécurité et la flexibilité. Dans ce contexte, ce projet vise à concevoir et développer un système de contrôle d'accès intelligent, basé sur l'unité Orduino et deux méthodes de vérification : un code secret unique (PIN) et une empreinte vocale. Le système utilise également des techniques d'intelligence artificielle pour améliorer la vérification de l'identité des utilisateurs et résister aux tentatives de falsification et d'imitation. Une application mobile a été développée pour permettre à l'administrateur de gérer l'enregistrement des utilisateurs autorisés. Un appareil intelligent, installé près de la porte, permet à l'utilisateur de saisir son code secret et son empreinte vocale en lisant la phrase unique générée. Il vérifie d'abord la correspondance entre le texte parlé et la phrase apparente, puis la correspondance avec la voix. Une fois la vérification réussie, un mot de passe chiffré est envoyé via Bluetooth à l'unité Arduino responsable de l'ouverture de la porte. Le système a été initialement testé sur un petit groupe d'utilisateurs et les premiers résultats ont montré une bonne efficacité, témoignant de son efficacité en conditions réelles, malgré quelques problèmes tels qu'une mauvaise prononciation et un niveau sonore élevé. Ce système se caractérise par un haut niveau de sécurité grâce à un mécanisme de double vérification, ainsi que par sa facilité d'installation et son faible coût par rapport à d'autres systèmes, ce qui en fait une solution pratique, flexible et évolutive pour répondre aux exigences de contrôle d'accès dans de nombreux environnements.

**Mots-clés :** Contrôle d'accès, Arduino, Voiceprint, Intelligence artificielle, Intelligence artificielle générative.

# Contents

General Introduction . . . . .	1
<b>Chapter 1: Generalities</b>	<b>3</b>
1.1 Introduction . . . . .	4
1.2 Access control system . . . . .	4
1.3 Types of Access Control Systems . . . . .	5
1.3.1 Logical Access Control Systems . . . . .	5
1.3.2 Physical Access Control Systems . . . . .	5
1.4 Traditional vs Smart Access Control Systems . . . . .	6
1.4.1 Traditional Access Control Systems . . . . .	6
1.4.2 Smart Access Control Systems . . . . .	7
1.5 Control board (Arduino) . . . . .	12
1.5.1 Types of Arduino control board . . . . .	12
1.6 Conclusion . . . . .	12
<b>Chapter 2: Overview of the Internet of Things and Related Work</b>	<b>13</b>
2.1 Introduction . . . . .	14
2.2 An overview of the Internet of Things . . . . .	14
2.2.1 Definition . . . . .	14
2.2.2 Applications of IoT . . . . .	14
2.2.3 IoT Sensors and components used in Access Control Systems . . . . .	17
2.2.4 IoT Benefits and Drawbacks . . . . .	23
2.3 Related Work . . . . .	24
2.4 Conclusion . . . . .	27
<b>Chapter 3: System design</b>	<b>28</b>
3.1 Introduction . . . . .	29
3.2 Problem Statement . . . . .	29
3.3 Objective of project . . . . .	29
3.4 Proposed Solution and System Architecture . . . . .	30
3.5 System Diagram . . . . .	31
3.5.1 Sequence diagram . . . . .	31
3.5.2 Flow Chart . . . . .	37
3.6 Conclusion . . . . .	38
<b>Chapter 4: Implementation and Results</b>	<b>39</b>
4.1 Introduction . . . . .	40
4.2 Development Environment . . . . .	40
4.2.1 Software Environment . . . . .	40
4.2.2 Hardware Environment . . . . .	42



4.3	IA Models Used in the Project . . . . .	45
4.3.1	ECAPA-TDNN . . . . .	45
4.3.2	Meta-Llama-3-8B-Instruct . . . . .	45
4.3.3	Wisper . . . . .	45
4.4	Systems Implementation and Interfaces . . . . .	46
4.4.1	User Enrollment and Multi-Factor Authentication Workflow . . . . .	46
4.4.2	Mobile Application Development . . . . .	49
4.4.3	Mobile Application Interfaces . . . . .	49
4.4.4	Electronic Lock Control Integration . . . . .	56
4.5	Experimentation Examples and Results . . . . .	58
4.5.1	Experimentation Examples . . . . .	58
4.5.2	Some of the sentence-voice matching results . . . . .	62
4.6	Conclusion . . . . .	63
	General conclusion . . . . .	64

# List of Figures

1.1	Different types of access control[3]. . . . .	4
1.2	Types of Access Control Systems [4]. . . . .	5
1.3	Pin tumbler lock [11]. . . . .	6
1.4	Typical RFID System [15]. . . . .	7
1.5	Types of biometric authentication [17]. . . . .	8
1.6	Diagram of a latent fingerprint identification pipeline [20]. . . . .	8
1.7	Face recognition framework. . . . .	9
1.8	Major five steps of an iris recognition system. . . . .	10
1.9	Matrix Keypad for OTP [29]. . . . .	11
1.10	Different types of Arduino control board . . . . .	12
2.1	Different types of agriculture applications for IoT [33]. . . . .	15
2.2	Different types of smart Cities applications for IoT [36]. . . . .	16
2.3	RFID reader with accessories [29] . . . . .	17
2.4	Fingerprint Sensor . . . . .	17
2.5	Voice Recognition Microphone [42]. . . . .	18
2.6	Infrared Sensor [44]. . . . .	18
2.7	Passive Infrared Sensor [46]. . . . .	19
2.8	Proximity Sensor [47]. . . . .	19
2.9	Arduino UNO . . . . .	20
2.10	Raspberry Pi . . . . .	20
2.11	Servo Motor . . . . .	20
2.12	Relay Module . . . . .	21
2.13	Electric lock [29]. . . . .	21
2.14	Display Screen LCD [32]. . . . .	22
2.15	Bluetooth Module HC-05 . . . . .	22
3.1	General Architecture . . . . .	30
3.2	Administrator Sequence Diagram. . . . .	32
3.3	Registration process Sequence Diagram. . . . .	33
3.4	Authentication user Sequence Diagram. . . . .	34
3.5	Coach role Sequence Diagram. . . . .	36
3.6	Member role Sequence Diagram . . . . .	37
3.7	Flow Chart Diagram . . . . .	38
4.1	Arduino UNO . . . . .	42
4.2	Relay Module . . . . .	43
4.3	Bluetooth Module HC-05 . . . . .	43
4.4	Wires . . . . .	44
4.5	Electric lock . . . . .	44

4.6	Login pages . . . . .	50
4.7	Register pages . . . . .	51
4.8	User Lists Interface . . . . .	52
4.9	Open door page . . . . .	53
4.10	Authentication page . . . . .	54
4.11	Verification page . . . . .	55
4.12	Hardware Wiring diagram . . . . .	57
4.13	Real Picture of Proposed System . . . . .	57
4.14	User recognised . . . . .	58
4.15	Access granted . . . . .	58
4.16	Coach recognition failed . . . . .	59
4.17	User not recognized . . . . .	60
4.18	Access denied . . . . .	60
4.19	Coach not present . . . . .	61
4.20	Sentence-Voice matching . . . . .	62
4.21	Sentence matching and voice mismatch . . . . .	62
4.22	Sentence matching and voice mismatch . . . . .	62

# List of Tables

2.1 Comparison of Security Systems . . . . . 27

# List of Abbreviations

- ( **IoT** ) Internet of Things
- ( **PACS** ) Physical Access Control Systems
- ( **LACS** ) Logical Access Control Systems
- ( **RFID** ) Radio Frequency Identification
- ( **NFC** ) Near Field Communication
- ( **PIN** ) Personal Identification Number
- ( **OTP** ) One-Time Password
- ( **BLE** ) Bluetooth Low Energy
- ( **PIR** ) Passive Infrared
- ( **IR** ) Infrared
- ( **LCD** ) Liquid Crystal Display
- ( **OLED** ) Organic Light-Emitting Diode
- ( **UML** ) Unified Modeling Language.
- ( **NumPy** ) Numerical Python.
- ( **HTTP** ) Hypertext Transfer Protocol
- ( **AI** ) Artificial Intelligence
- ( **LLM** ) Large Language Model
- ( **ECAPA-TDNN** ) Emphasized Channel Attention and Pooled Attention Time-Delay Neural Network

# General Introduction

Access control systems play a vital role in protecting both physical and digital assets by ensuring that only authorised individuals can access specific areas, resources, or sensitive information. In modern environments such as corporate offices, data centres, hospitals, government buildings, and industrial facilities, effective access control is crucial to maintaining operational security, protecting data, ensuring user accountability, and meeting regulatory compliance standards. These systems represent the first line of defence against unauthorised access, theft, sabotage, and other forms of intrusion.

Despite significant advances, many facilities still rely on traditional methods such as physical keys, PIN codes, or magnetic cards. Although simple and cost-effective, these methods suffer from serious limitations in terms of security, scalability, and user convenience. For example, PINs are vulnerable to guessing, sharing, or observation through shoulder surfing or phishing, and they do not offer a guarantee of the actual identity of the user. In addition, traditional systems often lack real-time monitoring, fine-grained permission control, and adaptive policy enforcement.

To overcome these challenges, biometric authentication systems have emerged, offering a more secure alternative utilising unique physiological or behavioural traits. However, even these systems are not entirely immune to attacks. Voice-based biometric systems, in particular, remain vulnerable to identity spoofing through recorded or synthetically generated voices. Furthermore, many existing solutions lack real-time verification or physical integration with access control devices, which limits their real-world applicability.

This project proposes a novel IoT-based access control system that tightly integrates biometric voice authentication with physical access mechanisms, such as gate unlocking. The proposed solution employs two-factor authentication: something the user knows (a PIN code), and something the user is (their voice). To further enhance security, the system uses generative artificial intelligence to produce a unique authentication phrase for each login attempt, which the user must read aloud. This dynamic phrase generation reduces the risk of replay attacks using recorded audio.

The authentication process consists of two key steps: verifying that the user accurately repeated the generated phrase and analysing the user's voice recorded to confirm their identity. This layered approach significantly improves the robustness of the system against attempts to impersonate.

The proposed system was implemented as a case study at a swimming pool entrance, a context that requires strict access control, especially to protect vulnerable users such as children. The system incorporates a contextual access database that enforces specific policies, such as requiring the presence of a coach for supervision when needed.

Overall, this project aims to develop a secure, scalable and cost-effective access control solution based on the latest advances in artificial intelligence and biometric authentication. The system combines real-time voice analysis with physical control via an Arduino module, offering a practical and modern alternative to traditional systems. Addressing contemporary security issues such as spoofing and audio forgery lays the foundation for future modular access control architectures adaptable across various sectors.

In the long term, the project envisions a modular and extensible framework that can serve as the basis for next-generation access control systems in various domains.

The dissertation is divided into four chapters, each of which focuses on a different component of the research. An overview of the chapters is given below.

### ***Chapter 1: Generalities about Access Control Systems***

This chapter provides a comprehensive overview of access control systems of both physical and logical types, with a review of the techniques used in their implementation, highlighting their pivotal role in protecting assets and information.

### ***Chapter 2: Internet of Things***

In this chapter, we will discuss an overview of the IoT, its application areas, etc. In addition, some previous work is related to our project.

### ***Chapter 3: System design***

This chapter focuses on the analysis and design of the proposed access control system based on the Unified Modelling Language (UML). The chapter includes a set of diagrams, including a class diagram, sequence diagrams, as well as activity diagrams, to clarify the structure of the system and the interactions of its components.

### ***Chapter 4: System implementation***

This chapter begins by introducing the development tools and techniques used, as this includes back-end and front-end tools, as well as the hardware adopted to implement the entry system. It also discusses the results obtained and reviews the main interfaces of the system.

### ***General Conclusion***

Finally, we will conclude with a general conclusion in which we summarise the results of our project.

# **Chapter 1**

## **Generalities**



## 1.1 Introduction

Access control systems play a crucial role in securing both physical spaces and digital environments by regulating who is allowed to access specific resources and under what conditions. As security needs have evolved, so have these systems, moving from traditional mechanisms such as mechanical keys and simple PIN codes to more advanced, smart technologies that incorporate biometrics, wireless communication, and Internet of Things (IoT) integration.

In this chapter, we explore the fundamental concepts of access control systems, present their main physical and logical categories, and examine the technologies that support them. We also highlight the transition from traditional to smart systems, emphasising the growing importance of integrating intelligent, adaptive authentication mechanisms to address modern security challenges.

## 1.2 Access control system

An access control system is a security mechanism designed to regulate and restrict access to resources, data, or physical locations based on predefined policies. These systems ensure that only authorised individuals can gain access by implementing authentication and authorisation processes. Access control has evolved from traditional methods, such as magnetic cards, electronic keys, and PIN codes, which, despite their effectiveness, remain vulnerable to loss or unauthorised duplication. In contrast, smart access control systems use advanced technologies like voice recognition, facial recognition, and fingerprint scanning to improve security, improve efficiency, and minimise breaches. Various access control models, including discretionary, mandatory, and role-based access control, are used to enforce security policies and prevent unauthorised access[1][2].



Figure 1.1: Different types of access control[3].

## 1.3 Types of Access Control Systems

Access control systems form a crucial element in protecting both physical spaces and digital environments. These solutions are broadly divided into two primary categories: Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS), as illustrated in Figure 1.2

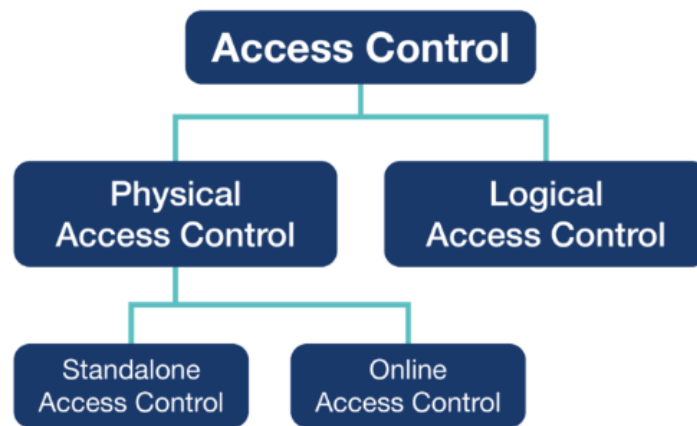


Figure 1.2: Types of Access Control Systems [4].

### 1.3.1 Logical Access Control Systems

- **Mechanisms and Functions :**

Logical Access Control Systems (LACS) manage user access to online resources such as databases, operating systems, and applications. They rely on various digital authentication methods, including passwords, two-factor authentication, and biometric identification. One widely used approach in LACS is Role-Based Access Control (RBAC), in addition to attribute-based or context-aware policies and Access Control Lists (ACLs). Standards such as XACML are implemented to ensure accurate and centralised access management [5].

- **Opportunities and Challenges :**

A key challenge lies in maintaining a balance between strong security and user accessibility, particularly in cloud-based or distributed environments. On the other hand, LACS offers significant opportunities by providing secure integration frameworks and enabling activity monitoring and analysis through AI-powered systems and cloud technologies [5].

### 1.3.2 Physical Access Control Systems

- **Mechanisms and functionality :**

Physical Access Control Systems (PACS) are responsible for managing who can enter physical locations and at what times. These systems typically use verification technologies such as RFID cards, biometric scanners, smart controllers, and card readers. Common components include electronic locks, control panels, and integrated alarm systems. PACS ensures secure access to buildings, rooms, and other physical infrastructure by verifying user identity through hardware-based mechanisms [6][7].

- **Obstacles and Prospects :**

Despite advances in PACS technology, research and development in this area remain limited compared to digital access control systems. One of the main challenges is integrating PACS with modern digital systems while maintaining compliance with strict security standards. However, PACS offer promising opportunities for innovation, particularly through policy-based access management, real-time event monitoring, and dynamic scheduling of access permissions [6][7].

## 1.4 Traditional vs Smart Access Control Systems

### 1.4.1 Traditional Access Control Systems

These systems rely on simple, manual methods without the use of smart technologies or internet connectivity.

- **Mechanical Keys and Locks**

According to [9], a mechanical key lock is a device used to protect a door or space where the construction and use of the mechanism are solely based on non-electronic components. It works through physical pieces that align with the pins in the lock cylinder, allowing direct access when the correct key is used [10], as illustrated in Figure 1.3.



Figure 1.3: Pin tumbler lock [11].

- **Security guards**

Security guards are professionals responsible for protecting people, property, and assets from various hazards in different environments [12]. Their responsibilities now extend beyond traditional duties, as they increasingly assist law enforcement by helping to prevent violations and crimes at work. As highlighted in [13], performing these duties effectively requires strong cognitive skills, adequate education, and structured training. These elements are crucial in shaping people who can respond quickly and responsibly within their legal limitations.

## 1.4.2 Smart Access Control Systems

These use modern technologies like IoT, biometrics, and wireless communication for enhanced security and flexibility.

- **RFID cards**

RFID technology is composed of an RFID tag and an RFID reader linked to a computer system. The tag is the part that collects real-time data and then transmits that data via radio waves. The tags usually have two parts, a small chip and an antenna. Information is stored and processed by the chip while the antenna is used to receive and transmit the information [14].



Figure 1.4: Typical RFID System [15].

- **Biometric authentication**

The term "biometrics" describes the process of identifying individuals by measuring and analysing their distinct physical or behavioural characteristics. Identification of people. It functions by comparing live data from people with pre-enrolled records. In real time. An 'enrollment' reader collects biometric data, which is then converted into a template. saved on a smart card or in an access control database. The data is protected from being decoded by the encoding. compared to a sample for a pass/fail outcome, but not replicated. The categorisation of biometric sensors as contact-based, involving physical touch, or contactless, which requires no touch. These Identification systems are made safer and more efficient by technology [16].

Access control systems only employ a few biometric identification methods, specifically those that Strike a balance between accuracy, speed, and expense. The most frequent types are as follows:



Figure 1.5: Types of biometric authentication [17].

**Fingerprint Recognition :** The main evidence consists of latent fingerprints and impressions. Two key uses of fingerprint matching in biometrics are listed below: latent fingerprint detection and fingerprint verification. The goal of fingerprint verification is to verify someone's identity. If a claimed identity and a fingerprint impression are provided, The provided impression is compared to a prior recorded impression by the verification algorithm. Returns a determination of a match or non-match based on the identity associated with that vision. On the other hand, The process of identifying latent fingerprints involves comparing impressions to a reference database. that are most like the latent fingerprint in question [18][19].

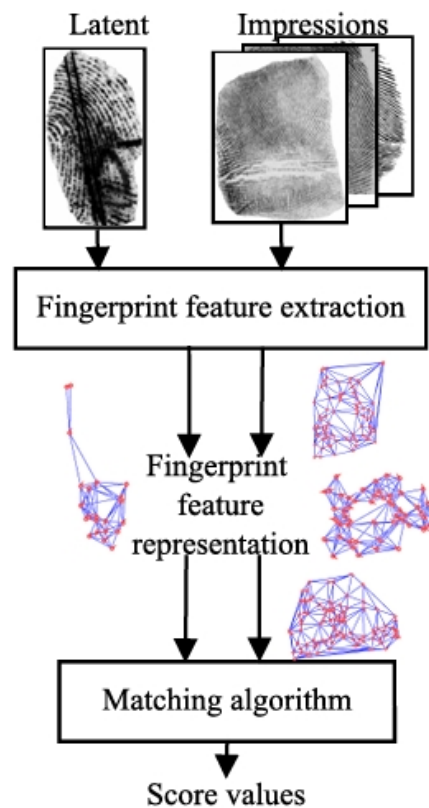


Figure 1.6: Diagram of a latent fingerprint identification pipeline [20].

**Face Recognition :** Face recognition technology [21] is a biometric method that identifies individuals based on facial features. It collects facial images and processes them automatically using recognition systems. As a subset of visual pattern recognition, it analyses image or video data composed of pixel matrices to determine identity. Key processes include face detection, facial feature positioning, identity recognition, and image pre-processing. Detection defines the coordinate system of all faces in an image, while positioning locates individual facial features usually with lower computational cost. The output can be square or rectangular. This technology is widely used in access control, security, and financial services, with increasing applications in other sectors.

Facial recognition systems [22] can be structured using a framework based on three main criteria: Modality (Unimodal or Multimodal), Dimensionality (2D or 3D), and Feature Quality (Physiological or Behavioral). This taxonomy supports model customization and selection in facial recognition tasks. As illustrated in Fig. 1.7, users can combine different attributes from each criterion depending on dataset availability, application-specific requirements, user preferences, system complexity, and time constraints. This flexible approach enables the design of recognition systems tailored to diverse operational contexts.

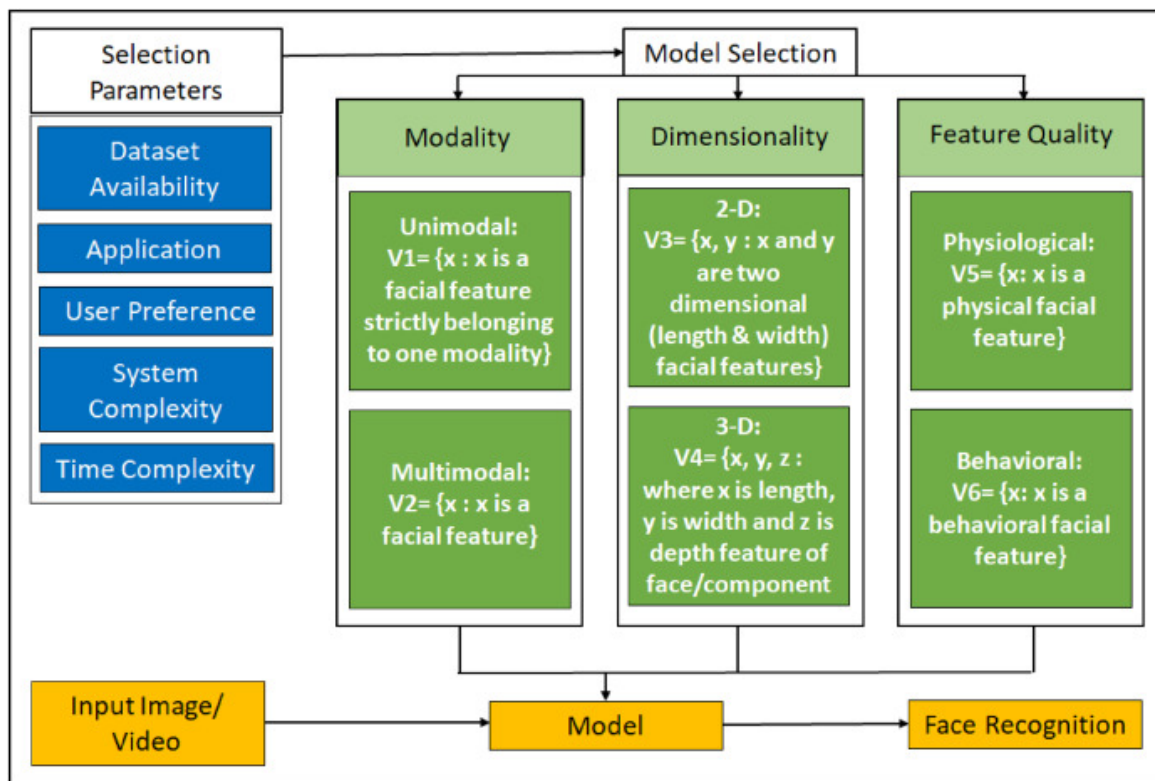


Figure 1.7: Face recognition framework.

**Iris Recognition :** The use of the human iris as a unique biometric trait has led to the development of a highly reliable and accurate identification technology. The iris is the ring-shaped region located between the pupil and the sclera (white of the eye). It has a complex structure and contains numerous texture features that are unique to each individual [23].

Iris recognition systems offer several advantages that enhance their effectiveness in real-world applications. These include the lifelong stability of iris patterns, their inherent randomness and complexity, uniqueness even among identical twins, and lower false match (FMR) and false reject rates (FRR) compared to other biometric methods. During the Covid-19 pandemic, a key feature gained importance: the ability to capture iris templates through contactless methods known as free touch biometrics from distances greater than half a meter.

A typical iris recognition pipeline consists of five stages: image acquisition, iris region segmentation, normalization, feature extraction, and matching [24]. Figure 1.8 illustrates these steps and how they are connected.

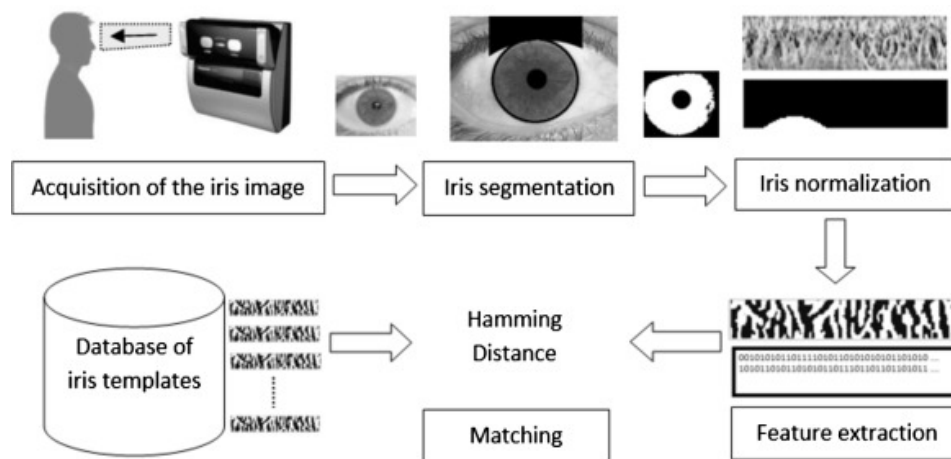


Figure 1.8: Major five steps of an iris recognition system.

**Palmprint or Hand Geometry :** As discussed in [25], palmprint or hand geometry biometrics are based on the geometric structure of the hand, where the human palm exhibits ridge patterns and valleys similar to those found in fingerprints. However, this method presents certain limitations. It is not well-suited for children, as the shape of the hand tends to change with age. Furthermore, it may be unreliable for people with arthritis, as proper placement of the hand on the scanner can be hindered.

**Voice Recognition :** Voice recognition is a broad field within artificial intelligence and signal processing that focuses on the analysis of human voice characteristics. Each individual has a unique voice signature, which can be captured and analysed by AI algorithms. The field is generally divided into two major subfields:

### 1- Speech Recognition:

Speech recognition is a complex process that involves the conversion of spoken language into text, utilising various statistical and mathematical models to handle the inherent variability of human speech. The technology has advanced significantly, with applications ranging from dictation to interactive voice response systems. The key components of modern speech recognition systems include acoustic-phonetic modelling, language modelling, and decoding techniques, which work together to accurately interpret speech[26][27].



## 2- Speaker Recognition:

As explained in [28], Speaker recognition focuses on identifying individuals based on the unique characteristics of their voice. Every person's voice is distinct due to physical traits such as vocal tract shape, larynx size, and other anatomical differences involved in sound production. Beyond these physical aspects, variations in speech style, pronunciation, and vocabulary also contribute to vocal uniqueness. As a result, voice can serve as a biometric identifier, alongside methods like fingerprinting and retinal scanning.

Speaker recognition is typically divided into two main tasks:

- *Speaker Verification* : Confirms whether a person's voice matches a claimed identity.
- *Speaker Identification* : Determines which individual is speaking from a known set of speakers.

- **QR code or OTP (One-Time Password)**

OTPs provide a dynamic and secure authentication method and are often used in conjunction with mobile devices to ensure that only authorised users can access.

QR codes can be used for quick contactless access and are suitable for temporary access or guest entry [29].



Figure 1.9: Matrix Keypad for OTP [29].

- **Cloud-based systems**

Facilitate centralised management of access control systems, allowing scalable and flexible solutions that can be easily updated and monitored. They also support various connectivity modules such as Bluetooth and NB-IoT to enhance connectivity and user experience [2].



## 1.5 Control board (Arduino)

An Arduino board [11] is a small (5.33 x 6.85 cm) electronic board equipped with a microcontroller. The microcontroller allows, from events detected by sensors to programming and controlling actuators, the Arduino board is therefore a programmable interface. The most widely used Arduino board is the ArduinoUno board.

### 1.5.1 Types of Arduino control board

Since 2007, there have been several iterations of the Arduino family, including the following: Arduino Uno (R3), Arduino Nano, Arduino Micro, Arduino Due Lily Pad Arduino Bluetooth Arduino 10,000 Arduino Red Board Mega (R3) Arduino Explorer Arduino zero..., As shown in Figure 1.10.

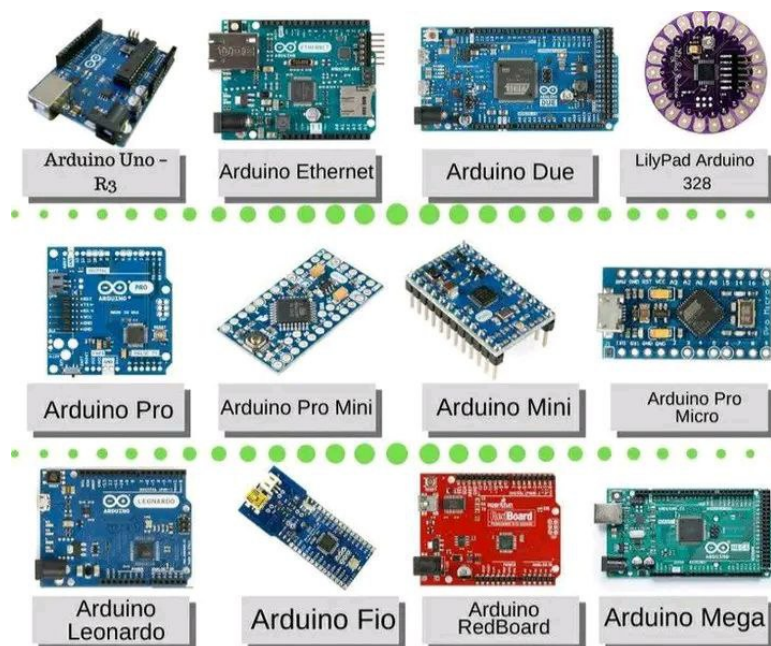


Figure 1.10: Different types of Arduino control board

## 1.6 Conclusion

This chapter covers the general principles of access control systems, providing a comprehensive definition and explaining their essential role in protecting physical and logical resources from unauthorized access.

## **Chapter 2**

# **Overview of the Internet of Things and Related Work**

## 2.1 Introduction

The idea of connecting devices to a network and controlling them remotely using smart devices from anywhere in the world is known as the Internet of Things (IoT). Today, IoT plays a key role in facilitating daily life and is widely applied across many sectors. In this chapter, we provide a comprehensive overview of IoT. First, we present its definition, application areas, and the various sensors and components used in access control systems. This is followed by an explanation of its advantages and disadvantages. Additionally, we highlight some recent related works in the context of our project.

## 2.2 An overview of the Internet of Things

In this part, we will highlight the IoT, its applications in different fields. Then we will present some components that can be used to achieve these systems.

### 2.2.1 Definition

The Internet of Things (IoT) refers to a vast network of interconnected physical objects that can collect and exchange data without requiring human interaction. These "things" are embedded with sensors, software, and various technologies that enable them to connect to the internet and communicate with other devices and systems [30]. This concept fundamentally transforms ordinary physical objects into smart devices capable of sensing their environment, processing information, and taking actions based on programmed rules or artificial intelligence algorithms.

According to [31], IoT extends internet connectivity beyond conventional computing devices (like computers and smartphones) to everyday objects, machines, and systems, creating an intricate web of interconnected entities. This interconnectedness allows for seamless data flow between physical objects and digital systems, bridging the gap between the tangible world and the virtual realm. The IoT ecosystem typically consists of four main components:

- Sensors/devices that collect data.
- Connectivity infrastructure that transmits the data.
- Data processing systems that analyse the information.
- User interfaces that allow human interaction with the system

### 2.2.2 Applications of IoT

The versatility of IoT technology has led to its implementation across numerous sectors. We will explain some of it below:

- **Smart Homes :** Smart home applications are a significant area of IoT implementation, offering various benefits and some limitations. The concept originated in the 1970s with the X10 protocol, which enabled device communication. Today, smart home IoT devices are used for monitoring environmental conditions, managing appliances, and controlling access. Home automation remains a central function of these systems. Devices equipped with IoT technology

improve convenience and operational efficiency. IoT sensors can also assist the elderly by automating device control and detecting falls using floor or camera sensors. The market continues to grow, with an expected CAGR of 10%

- **Agriculture :** The Internet of Things (IoT) plays a pivotal role in advancing smart agriculture by integrating with Wireless Sensor Networks, enhancing production efficiency and resource distribution. Smart sensors monitor soil moisture, temperature, and humidity, transmitting real-time data to control centres to support informed decision-making. IoT is applied in smart irrigation systems to minimise water waste and detect pests and diseases at early stages. Communication protocols like ZigBee and LoRaWAN enable efficient data transmission across large agricultural areas. IoT also supports fertiliser optimisation by analysing soil nutrients and recommending ideal timing and quantities. Additionally, it aids in monitoring energy usage and improving power efficiency in farming operations. These applications promote sustainable agriculture, reduce costs, and maintain crop quality [34].

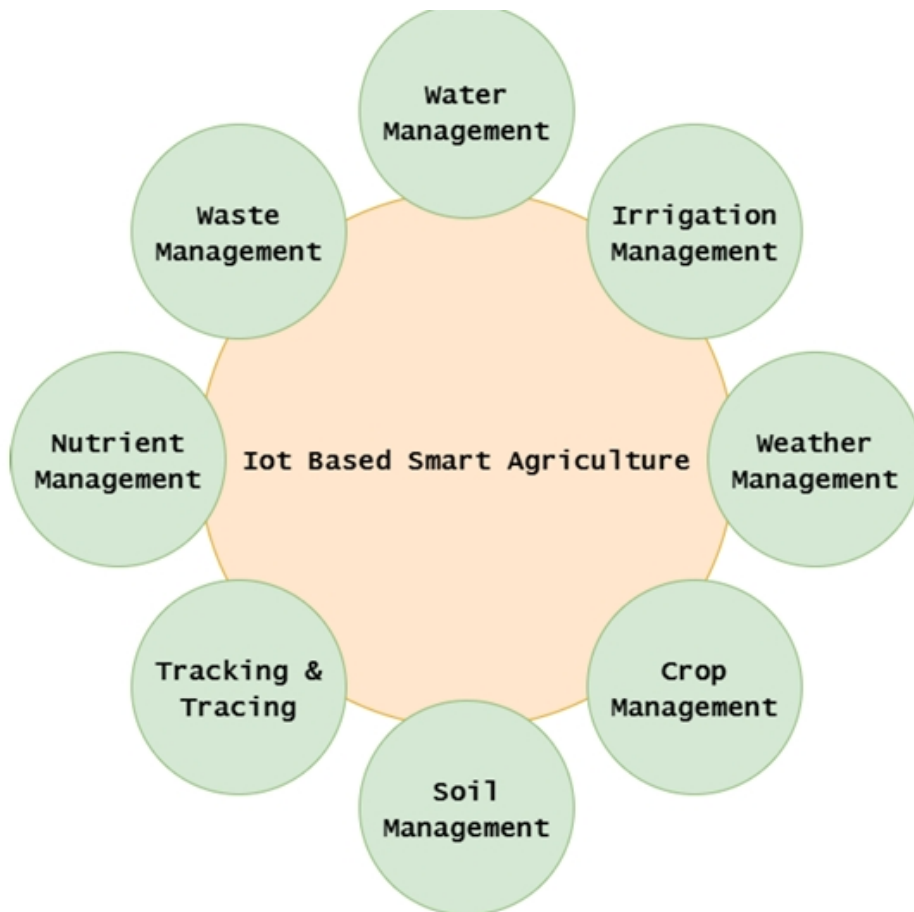


Figure 2.1: Different types of agriculture applications for IoT [33].

- **Smart Cities** : As part of the smart city vision, urban areas are increasingly adopting Internet of Things (IoT) solutions to enhance public services such as traffic management, waste collection, public safety, and environmental monitoring. Urban traffic systems use sensors and GPS-equipped vehicles to monitor congestion and guide drivers efficiently. In waste management, smart bins detect their fill levels and transmit data to control centres to optimise collection routes. Noise sensors are employed to monitor sound levels and detect public safety incidents like fights or glass breaking. Air quality sensors are deployed in parks and crowded areas to track pollution and provide health-related data to citizens. Smart lighting systems adjust street-lamp brightness automatically based on pedestrian presence and weather conditions to save energy. These technologies enable continuous monitoring and dynamic interaction between infrastructure and residents. Through such innovations, cities aim to improve quality of life while reducing operational costs [35]. The figure 2.2 below shows the different types of Internet of Things (IoT) applications in smart cities.

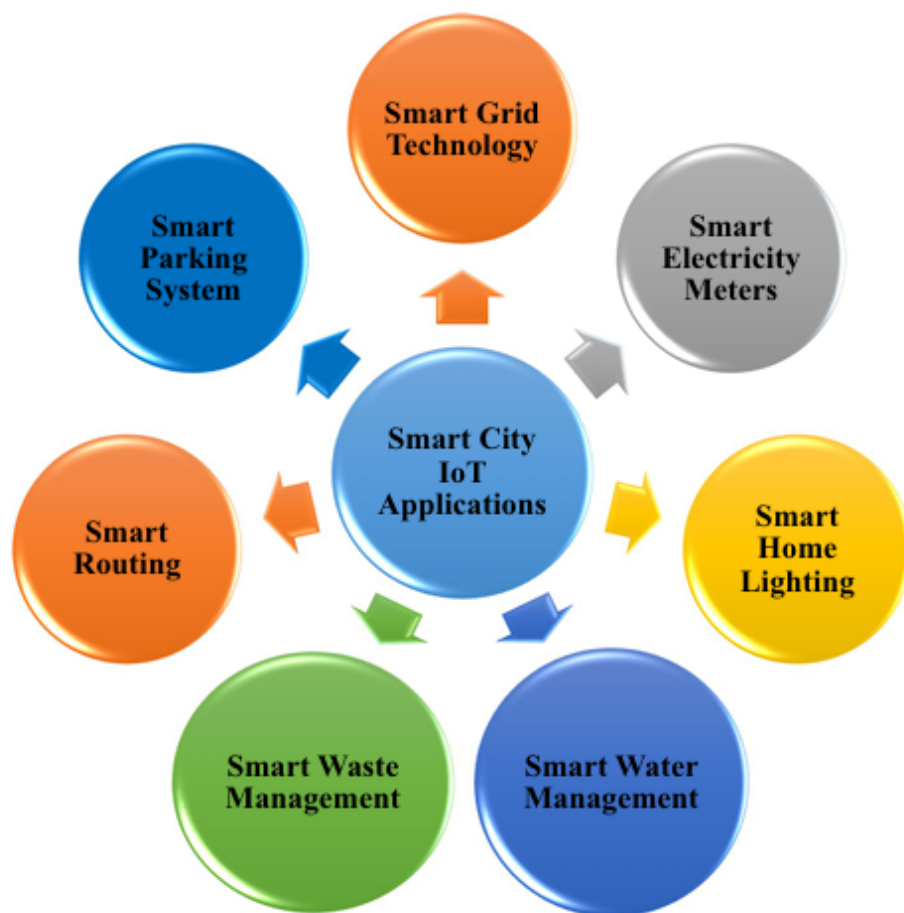


Figure 2.2: Different types of smart Cities applications for IoT [36].

- **Wearables** : As discussed in [37], Wearables are smart electronic devices that can be worn on the body, such as smart glasses, smartwatches, smart bracelets, and smart shoes. These devices are commonly used to monitor patient parameters, track usability, and assist in the care and monitoring of the elderly.

### 2.2.3 IoT Sensors and components used in Access Control Systems

Different types of sensors and components can commonly be used to develop an access control system.

#### a. Sensors

There are many types of sensors, typically:

- **RFID / NFC Reader :** RFID (Radio Frequency Identification) is an automatic identification technology that uses electromagnetic fields to detect objects carrying tags when near a reader. It operates over multiple radio frequencies with various tag types, some passive and others active. Passive RFID tags contain no internal power and respond only by backscattering signals from the reader. NFC (Near Field Communication) is a short-range wireless communication standard based on RFID, operating at 13.56 MHz and typically within 10 cm. It was chosen for ease of implementation, low power use, and enhanced security. NFC involves an initiator that generates an RF field and a passive target, and is widely used in contactless payments and peer-to-peer communication [38].

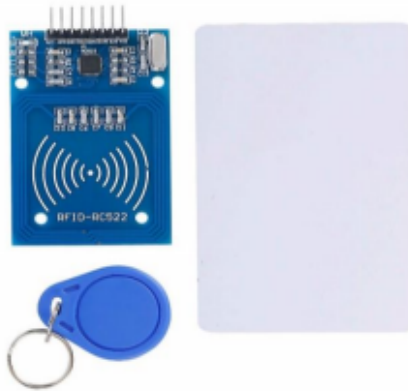


Figure 2.3: RFID reader with accessories [29]

- **Fingerprint Sensor :** A fingerprint sensor is a device used for identifying individuals by analysing the unique patterns of ridges and valleys on their fingerprints. These biometric devices capture unique fingerprint patterns through optical or capacitive scanning technologies. Modern fingerprint sensors incorporate liveness detection to prevent spoofing attempts using artificial fingers [39].



Figure 2.4: Fingerprint Sensor

- **Voice Recognition Microphone:** The microphone is used to convert the user's spoken commands into electrical signals, which are then sent to the voice recognition module. This system uses the V3 voice recognition module, a compact and user-friendly board designed to recognise and respond to voice commands. It supports up to 80 voice commands and can handle 7 commands simultaneously. Additionally, any voice can be trained to act as a command. Before recognising specific voice inputs, the module must first be trained with those commands [41].



Figure 2.5: Voice Recognition Microphone [42].

- **Infrared (IR) Sensor :** A passive infrared sensor identifies the heat signatures that people produce. and fauna. Infrared beams are projected and disruptions are detected by active IR sensors, which makes them helpful for determining if someone is coming closer to or is there at a door [43].

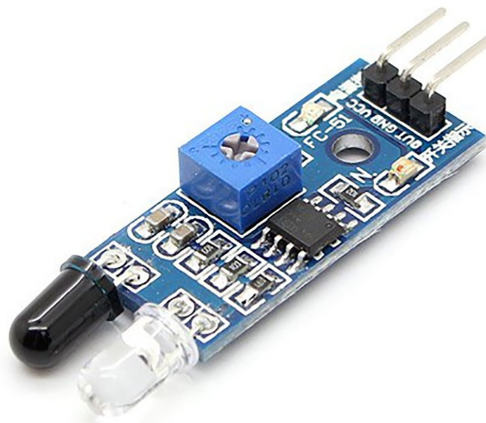


Figure 2.6: Infrared Sensor [44].

- **Facial Recognition Camera :** High-definition cameras are combined with sophisticated computer vision. Individuals are recognised using facial characteristics via vision algorithms. These systems examine a variety of facial points and capable of functioning in a variety of lighting situations, with more recent versions including 3D sensing for improved security [40].



- **Passive Infrared Sensor (PIR) :** Pyroelectric infrared (PIR) sensors are commonly used in occupancy detection and human tracking systems due to their low cost, power efficiency, and compact size. Their unobtrusive nature makes them suitable for privacy-sensitive environments. Dense arrays of PIR sensors combined with Fresnel lenses enable the detection of motion, identification of individuals, and counting of people entering or exiting spaces. In addition to presence detection, the analog output of these sensors provides information on movement speed, direction, distance, and body characteristics. This rich signal data can be exploited to enhance indoor human tracking and localisation applications [45].



Figure 2.7: Passive Infrared Sensor [46].

- **Proximity Sensor :** These devices utilise electricity to identify surrounding items without making physical contact. Infrared light, sound waves, or electromagnetic fields. They may be used to detect access control. The first step is to initiate the following authentication procedures [30].



Figure 2.8: Proximity Sensor [47].



### b. Components / Actuators

There are many types of Components typically:

- **Raspberry Pi / Arduino** These programmable computing platforms serve as the "brain" of IoT access control systems. Raspberry Pi offers more computing power suitable for complex applications like facial recognition, while Arduino provides efficient control for simpler systems. Both platforms support various connectivity options and can interface with multiple sensors [48].

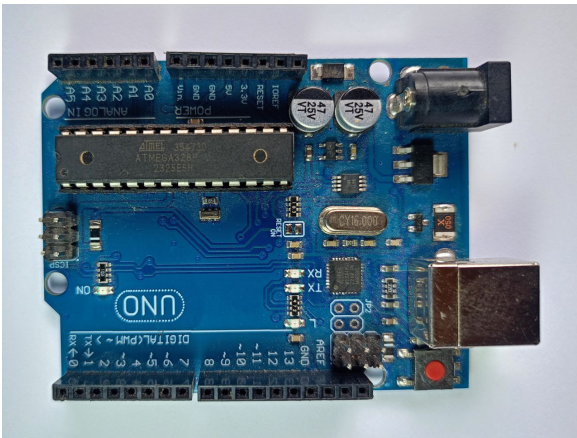


Figure 2.9: Arduino UNO

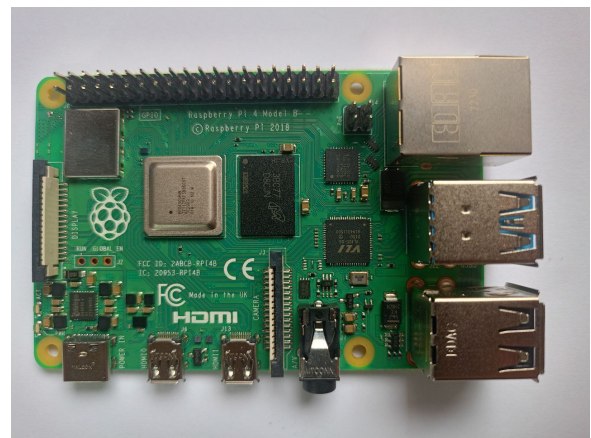


Figure 2.10: Raspberry Pi

- **Servo Motor** These precision motors provide controlled rotational movement for operating door locks, gates, or barriers. Their precise angular control allows for smooth, reliable operation of physical security mechanisms [31].



Figure 2.11: Servo Motor

- **Relay Module** A relay is an electronically controlled switch that works similarly to a light switch on a wall that is used to turn a light on or off. The relay is used to turn on or off other devices, such as electric door locks, alarm bells, whistles, turning on lights, turning on digital communication devices, and many other uses.

One relay is usually used to control the electric door lock, while other relays, commonly known as auxiliary relays, are used as needed. When the relay is activated or stopped, the device to which it is connected is automatically switched on or off. [7].

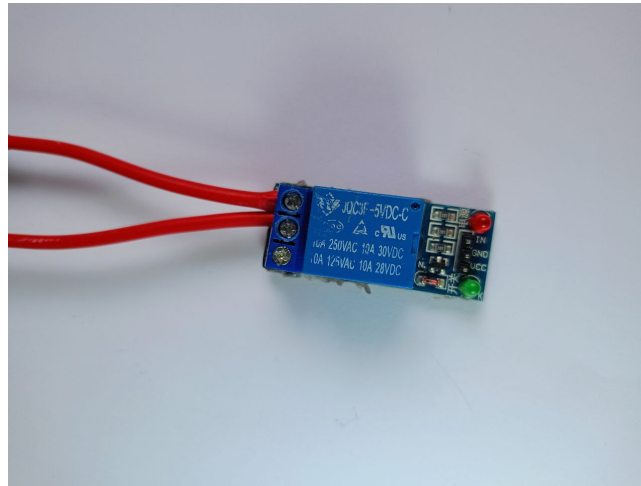


Figure 2.12: Relay Module

- **Solenoid Electric** The electrical opening and latch lock mechanism shown in the image refers to a solenoid lock. This is one of the most common types of electromagnetic locks. When the lock is activated, electric current flows through the coil, generating a magnetic field that pulls back a metal plunger or locking pin, thereby unlocking the device [29].

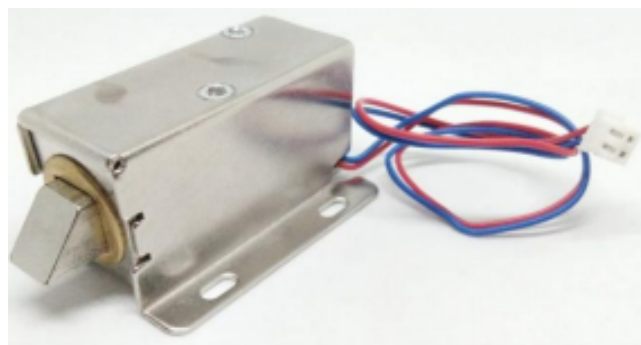


Figure 2.13: Electric lock [29].

- **Camera Module** Dedicated camera units capture images or video for facial recognition, surveillance, or visitor identification. High-definition cameras with infrared capabilities enable operation in low-light conditions [30].
- **Display Screen (LCD/OLED)** These components provide visual feedback to users about system status, authentication results, or instructions. Modern systems may incorporate touchscreen displays for interactive user interfaces [31].



Figure 2.14: Display Screen LCD [32].

- **Wi-Fi Module**
- **Bluetooth Module (e.g., HC-05)** These components enable short-range wireless communication between mobile devices and access control systems. Bluetooth Low Energy (BLE) variants offer energy-efficient connectivity for battery-powered applications [30].

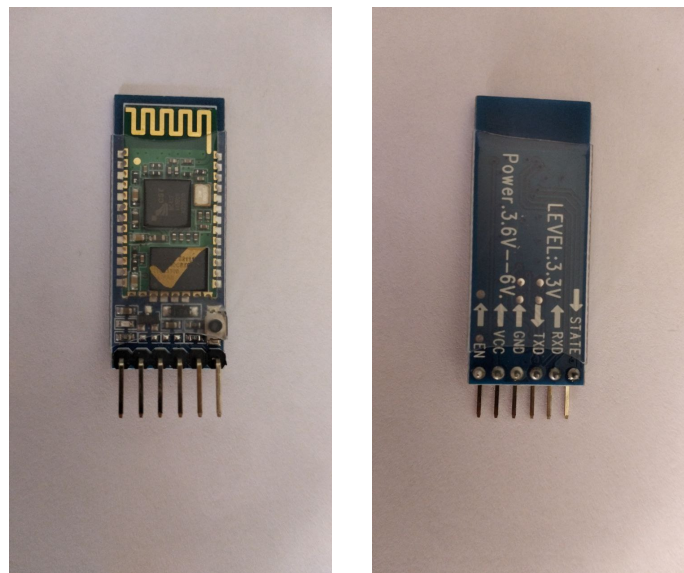


Figure 2.15: Bluetooth Module HC-05

### 2.2.4 IoT Benefits and Drawbacks

IoT offers numerous advantages to the users, as well as has many disadvantages which are presented below [50]:

- **Benefits:**

**Minimizing the human effort :** IoT devices communicate and interact with each other, they provide automation of the tasks which helps us to improve the quality of business services and reduce the need for human intervention.

**Save time :** As we discussed above it reduces human effort, so it saves a lot of our time also. Saving time is the primary advantage of an IoT platform.

**Enhanced data collection :** In IOT, Information is very easily accessible, even if we are away from our location, and it is updated very fast in real time. So these devices can access any information from any place at any time on any device.

**Improved security :** As we know in IOT, if we have a system that is interconnected, it can assist in the smarter control of cities and homes through mobile phones. It enhances security and offers us personal protection.

- **Drawbacks:**

As IoT provides advantages, it also has a significant set of drawbacks. Some disadvantages of IOT are given below:

**Security issues :** IoT systems communicate and connect over networks. So, they offer little control despite any security measures, and they can invite various kinds of network attacks.

**Privacy concern :** The IoT system provides personal data in detail without the user's active participation.

**The complexity of the system :** Developing, maintaining, designing, and enabling the extensive technology to IoT system is a quite complex process.

**High chances of the entire system getting corrupted :** It may be possible that every connected device will become corrupted if there is a bug in the device.

**High dependency on the internet :** heavily relies on the internet and cannot function effectively without the internet.

## 2.3 Related Work

Agarwal et al propose an innovative IoT-based security system called the HSDL System, which integrates smart door locking with home security functionalities for enhanced protection and convenience. The system allows users to lock and unlock doors remotely via a mobile app using Bluetooth or internet connectivity. A motion detection mechanism, powered by Passive Infrared (PIR) sensors, distinguishes between household members, visitors, and potential intruders. The system captures visitor images and emails them to the homeowner, while intrusion attempts trigger alarms and alert notifications. A Raspberry Pi 3 is the central controller, managing all hardware components, including an electromagnetic lock for enhanced security. Designed to overcome the limitations of traditional security systems, this cost-effective solution enhances both ease of use and surveillance efficiency [51].

### Synthesis

- The integration of IoT technology ensures a smart, automated security solution for homes.
- Real-time alerts and image capturing enhance security awareness and response capabilities.
- The study demonstrates that the system effectively differentiates between users, visitors, and intruders, improving its reliability.
- The system's effectiveness has only been evaluated through simulations, which necessitates real-world testing to confirm its resilience against advanced intrusion techniques.
- The potential for cybersecurity threats is not extensively addressed in the paper.
- Motion detection alone may not always be accurate, potentially leading to false alarms.

In [52], the authors present a biometric-based security system utilising face recognition for access control. The system employs Principal Component Analysis (PCA) for facial recognition due to its efficiency in reducing data dimensions and robustness to noise. The system is implemented using MATLAB for image processing and an Arduino UNO microcontroller for controlling access. The process involves capturing an individual's image via a webcam, comparing it with a pre-stored database, and granting access if the face is recognised. The system ensures secure authentication by eliminating traditional vulnerabilities like stolen passwords or access cards. Performance evaluations demonstrated that PCA improves recognition speed and reduces errors under controlled conditions, making it a viable solution for real-time security applications.

### Synthesis

- This system offers a secure and efficient biometric authentication method for access control.
- The use of PCA improves recognition speed but may suffer from accuracy limitations under varying lighting conditions.
- One drawback is the dependence on MATLAB, which may limit real-world deployment due to processing constraints.
- The system's Arduino UNO microcontroller has limited processing power, making it unsuitable for large-scale applications without hardware upgrades.

Andreas et al introduce a smart door security system utilising ESP32 and IoT (Internet of Things) to enhance home security and enable remote access control. The system allows users to monitor door status, manage access remotely, and receive security alerts via an Android mobile application. The system employs the MQTT protocol with SSL encryption to ensure secure communication between the smartphone and the door lock mechanism. A PIR motion sensor detects movement near the door, while a touch sensor on the door handle identifies physical interaction. If the door is forcibly opened, an alarm is triggered, and a notification is sent to the homeowner, alerting them to a potential security breach. Performance evaluations demonstrated that the motion sensor accurately detects movement up to 1.6 meters, and all communications are encrypted, ensuring secure message transmission [53].

### **Synthesis**

- This system provides a cost-effective and IoT-powered home security solution, offering real-time monitoring and remote access.
- Its reliability and security could be further enhanced by integrating biometric authentication, backup power, and emergency response features.
- One limitation is the PIR sensor's limited detection range of only 1.6 meters, which may create blind spots where intrusions could go undetected
- The system relies on magnetic and touch sensors, which could potentially be bypassed using external tools, posing a security risk

Morkat et al present a two-level security door access system combining keypad authentication and voice recognition for enhanced security. A matrix keypad connected to a microcontroller handles first-level authentication by verifying a password. If correct, the system proceeds to second-level authentication using a voice recognition module (HM2007). A tri-state buffer manages data flow between the microcontroller and the DSP chip in the voice module.

Tests showed that optimal voice recognition occurs within 1.0 cm to 16.0 cm in quiet conditions but drops to 1.0 cm to 6.0 cm in noisy environments. Gender-based recognition bias was observed, and no cybersecurity measures were included to prevent spoofing or hacking. Despite these limitations, integrating both keypad and voice authentication strengthens access control [54].

### **Synthesis**

- The combination of keypad authentication and voice recognition enhances security, making unauthorised access more difficult.
- The system is user-friendly and provides a dual-layer authentication process, increasing reliability for high-security environments.
- The experimental results show that the system performs well in noiseless conditions, especially when the user speaks at an optimal distance from the microphone.
- The system's accuracy decreases significantly in noisy environments, which affects its overall performance.
- High hardware cost: The system requires multiple components, including a microcontroller, keypad, voice recognition module (HM2007), tri-state buffer, and DSP chip, which increases the overall cost compared to simpler authentication methods like RFID or PIN-only access.

In [55], the authors explore advanced techniques in speaker recognition, leveraging deep learning to enhance the accuracy and efficiency of voice authentication systems. The system processes speech signals and extracts distinctive features from individuals' voices, enabling precise speaker differentiation. This is achieved using deep learning models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which analyse speech patterns and extract deep features from audio recordings. The implementation of these techniques relies on powerful hardware and software tools. High-performance GPUs are used to accelerate deep learning computations, while frameworks like TensorFlow, PyTorch, and Keras provide robust environments for training and deploying speaker recognition models. Additionally, autoencoders, x-vector, and d-vector methods are utilised for feature extraction and representation learning. Speech data is processed using signal processing libraries such as Librosa and Kaldi, ensuring effective feature extraction and preprocessing. These technologies collectively enhance the system's ability to recognise speakers with high accuracy, even in challenging environments.

### Synthesis

- The effectiveness of these systems is validated through extensive experiments using various speech databases, demonstrating superior accuracy compared to traditional methods. Additionally, the study discusses challenges faced by speaker recognition systems, such as the impact of environmental noise and variations in speech due to emotional or health conditions. The paper also highlights recent advancements, including x-vector and d-vector techniques, which have significantly improved speaker recognition performance in non-ideal conditions.
- However, some limitations remain:
  - The model requires large amounts of training data.
  - Performance drops in noisy environments.
  - High computational power (GPUs) is needed.
  - The decision-making process is not interpretable.
  - Vulnerable to deepfake and replay attacks.
  - Struggles with unseen accents and languages.

In [56], the authors propose an Examination Hall Entry Control System using Radio Frequency Identification (RFID) technology to ensure secure and efficient student authentication. The system integrates Arduino as the main processing unit, an RFID reader and tags for authentication, and a web-based application for monitoring and managing examination attendance records. The RFID reader scans a student's RFID card and verifies it against a database, granting access if the student is registered. The system reduces manual verification efforts by 73 percent and decreases entry time by 35 seconds per student compared to traditional methods. Microsoft SQL Server is used for database management.

### Synthesis

- Prevents unauthorised students from entering, enhancing security.
- Reduces verification time and speeds up the entry process.
- Provides real-time attendance tracking via a web application.
- Harder to manipulate compared to traditional paper-based lists.

- However, some limitations remain:
  - RFID cards can be lost or stolen, leading to unauthorised access.
  - Requires purchasing and maintaining RFID readers, increasing costs.
  - Lacks biometric verification, reducing authentication accuracy.
  - Limited reader range may cause congestion at entry points.

Paper	Mobile App	Camera Usage	Smart System	IoT Integration	Deep Learning	Sensor Used	Cost
[51]	Yes	Yes	Yes	Yes	-	Yes	Low
[52]	-	Yes	-	-	-	Yes	Medium
[53]	Yes	-	Yes	Yes	-	Yes	Low
[54]	-	-	Yes	-	-	Yes	Medium
[55]	-	-	Yes	-	Yes	-	Very High
[56]	-	-	-	-	-	Yes	Low

Table 2.1: Comparison of Security Systems

The table 2.1 presents these research papers and articles that propose different solutions and technologies for enhancing security and access control systems. Some utilise the Internet of Things for smart lock control, while others rely on facial or voice recognition for identity verification. Deep learning techniques are also employed to analyse voice patterns and improve recognition accuracy. All of them aim to enhance security, improve the efficiency of access systems, and provide reliable solutions to protect against security threats.

## 2.4 Conclusion

In this chapter, we discussed related papers that propose similar solutions and approaches to addressing security challenges and ensuring authorised access. In the next chapter, we will talk about how we conceptualised our solution, architecture and related subsystems.



## **Chapter 3**

### **System design**

## 3.1 Introduction

System design is a critical phase in software development that defines the infrastructure, components, interfaces, and data required to meet specific system requirements. This chapter presents the design methodology of our system. The design process involves analysing user requirements, creating appropriate diagrams, and defining the system architecture to ensure optimal performance, robust security, and a user-friendly experience.

## 3.2 Problem Statement

Despite the continuous advancements in access control systems, many facilities still rely on traditional methods such as physical keys, personal identification numbers (PIN), or magnetic cards. These methods have proven to be limited in terms of security and efficiency, as they are prone to loss, theft, or unauthorised duplication. Furthermore, the sharing of access credentials among users poses a serious security threat to facilities. Card-based systems also require physical items that can be lost or stolen, and these traditional solutions involve higher operational costs and longer times for distribution, replacement, and management.

Although biometric authentication systems have emerged and demonstrated their effectiveness in this field, they are not immune to breaches, especially those based on voice recognition. Many such systems rely on simplified technologies, such as fixed passphrases or voice recognition alone, without verifying the actual presence of the individual, making them vulnerable to identity spoofing attacks using recorded or synthetically generated voices. Moreover, many currently deployed voice authentication systems lack actual integration with physical access control devices, such as door opening mechanisms, which limits their practical applicability.

This has led to a growing need in the security sector for an access control system that is robust, cost-effective and fast to implement and that keeps up with modern security challenges and reduces the dependence on traditional methods.

## 3.3 Objective of project

- Design an intelligent access control system based on the Internet of Things (IoT) technologies, fully integrated with physical control components such as Arduino, relays, and electric locks.
- Replacing traditional systems such as keys and access cards with a more reliable, cost-effective, and easier-to-manage solution.
- Providing a practical and low-cost solution relative to the level of security it offers, with easy deployment in various environments such as laboratories, gym halls, private offices, and swimming clubs.
- Enhancing security through advanced voice authentication techniques that prevent unauthorised access and reduce the risk of identity theft or spoofing, while developing a system that addresses modern security challenges, particularly in voice-based authentication.
- Utilising high-precision audio processing technologies with extremely low error rates.
- Deploying and evaluating the system in real-world semi-public environments such as pools and gyms to assess its effectiveness and ease of use.

### 3.4 Proposed Solution and System Architecture

The proposed system offers a modern solution powered by Internet of Things (IoT) technology for secure and effective access control. It has been designed specifically for places that require high protection and precise control over who is allowed to enter, such as swimming pools, gyms, and laboratories, whether in hospitals or universities.

The system features real-time interaction between authentication processes and the physical mechanisms of doors, where security is enhanced by adopting two-factor authentication. Initially, the user must enter a valid PIN. When validated, the system automatically generates a unique sentence, which the user must read aloud. Advanced voice processing and recognition algorithms are then used to verify that the voice matches the user's identity and that the spoken sentence matches the generated sentence. Only when all three conditions are met: (1) the PIN is correct, (2) the sound matches one of the pre-recorded sounds, and (3) the spoken sentence matches the generator, does the system send a command to the Arduino controller to open the door.

To embody this concept, a mobile application for the administrator was designed, enabling him to register users (including their data and voice recording), in addition to displaying the information of all registered users, whether they are members or swimming coaches. Another feature of the application is that administrators can open the door directly through the application, without having to undergo verification processes, as the owner of the facility or its highest official.

As for users, a multi-functional device has been allocated that is installed next to the door, featuring a screen to display the generated sentence and a built-in microphone to capture the user's voice while pronouncing it. This device allows the user to enter the password first, then read the voice sentence directly, after which the verification process takes place automatically, and the door opens automatically when all authentication conditions are met by a microcontroller (Arduino) programmed to receive opening commands via a wireless communication protocol (Bluetooth or WiFi).

The general architecture of the proposed system is shown in Figure 3.1

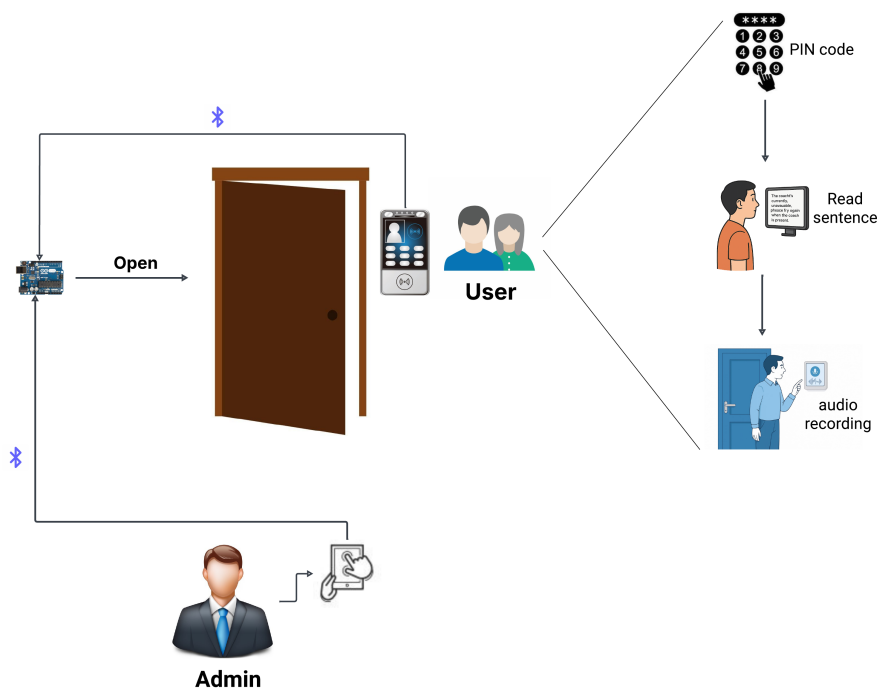


Figure 3.1: General Architecture

## 3.5 System Diagram

This section presents the system diagrams that illustrate how different components of the system interact with one another. These diagrams are essential for understanding the overall architecture, communication flow, and the sequence of operations within the system.

### 3.5.1 Sequence diagram

For a greater understanding of the system, the sequence diagram will be the appropriate tool to use. We shall delve deeply into the process explanation in the following context.

#### Sequence Diagram of Administrator

Figure 3.2 illustrates the interaction between the Administrator and the system during the use of the application, beginning with the log-in process and extending to various system functionalities. The diagram shows how messages are exchanged over time between the user and system components, providing a clear understanding of the logical flow of operations.

- When the administrator launches the application, the log-in page appears. They enter their email and password. The system first validates the input, particularly the email format, before proceeding with authentication using the Firebase database. If the credentials are correct, the system navigates directly to the application's home page.
- Otherwise, if the email or password is incorrect, an error message is displayed, prompting the administrator to verify the information and try again. This verification step ensures the security of the application.
- Once successfully authenticated, the system presents the main interface, allowing the administrator to choose from several options, such as viewing the list of coaches, members, or users currently inside the pool. Depending on the selected option, the corresponding list is displayed (e.g., list of coaches, members, or real-time logged-in users).
- If a new user, such as a member or coach, needs to be added to the system, the administrator can initiate the registration process. This is represented in Figure 3.1 as a referenced subprocess (ref: Registration process), which handles the collection of personal data and voice input.
- Beyond user management, the administrator also has the authority to control door access. The application sends a request to the Arduino microcontroller, which then triggers the relay responsible for opening the door without requiring verification.

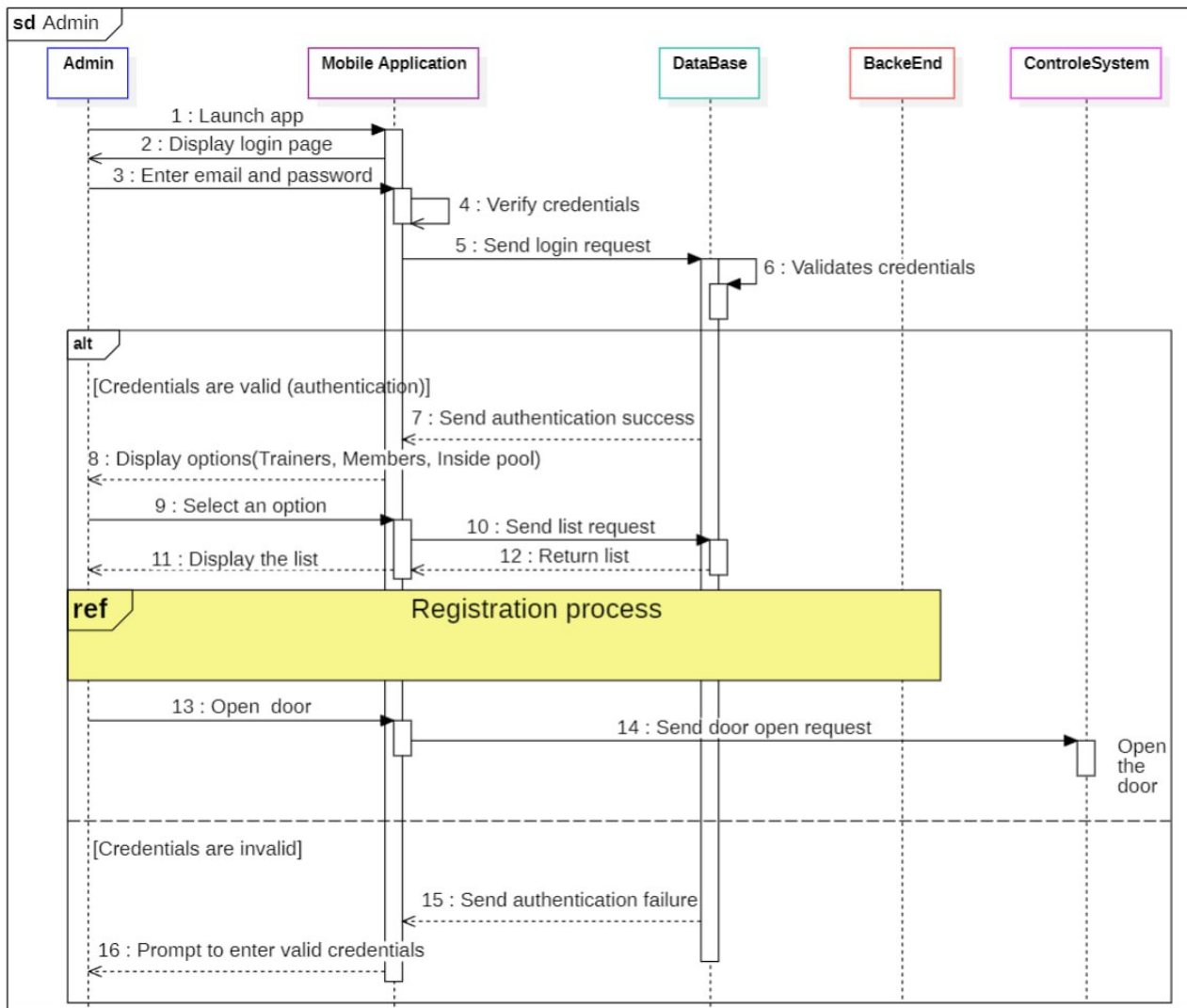


Figure 3.2: Administrator Sequence Diagram.

### Sequence Diagram of Registration process

Figure 3.3, which is referenced as a subprocess within Figure 3.1, provides a detailed view of the user registration process. The process involves the following steps:

- The administrator initiates the registration of a new user through the mobile application by entering their personal information and recording two voice samples.
- The user data, along with the two voice recordings, is then transmitted to the backend, where a unique PIN code is generated for the user. This PIN serves both as an identifier and as a reference for verification.
- Voice recordings undergo pre-processing, including silence trimming and noise reduction, to enhance their quality.
- Subsequently, voice features (also known as voice embeddings) are extracted from the processed recordings, and their average is computed. This step is crucial for the future identification and verification of the user.

- The system then stores the PIN code, user information, and the extracted voice features in the Firebase database to ensure centralised access and long-term storage.
- A confirmation message, along with the generated PIN code, is sent back to the mobile application to indicate successful registration.
- Finally, the application displays the generated PIN code to the administrator, confirming that the user has been registered successfully.

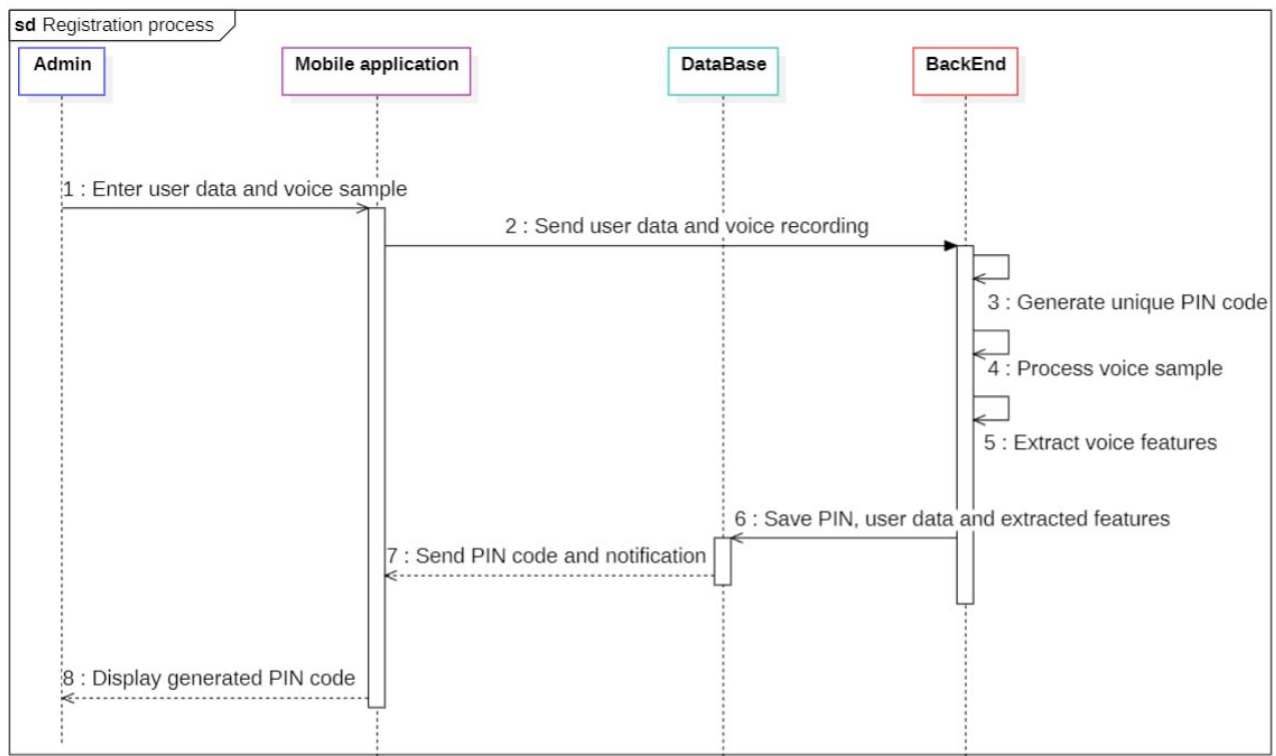


Figure 3.3: Registration process Sequence Diagram.

### Sequence Diagram of Authentication user

The sequence diagram shown in Figure 3.4 illustrates the two-factor authentication process, a critical and sensitive stage to ensure the security of the facility. It is at this point that individuals are either granted or denied access, based on their identity and system rules.

- The process begins when the user arrives at the door and interacts with a device mounted beside it (equipped with a screen and voice input support for voice authentication) through the login page. The user enters the personal identification number (PIN) obtained during the registration phase, which initiates the first authentication stage.
- Upon validating a correct PIN, the system identifies the user's role, either a swimming coach or a member.
  - Coaches are directed to the second authentication stage (detailed in Figure 3.4).

- Members, on the other hand, are only granted access if a coach is already present inside the facility (detailed in Figure 3.5).
- If the PIN is invalid, the system informs the user and prompts them to retry.

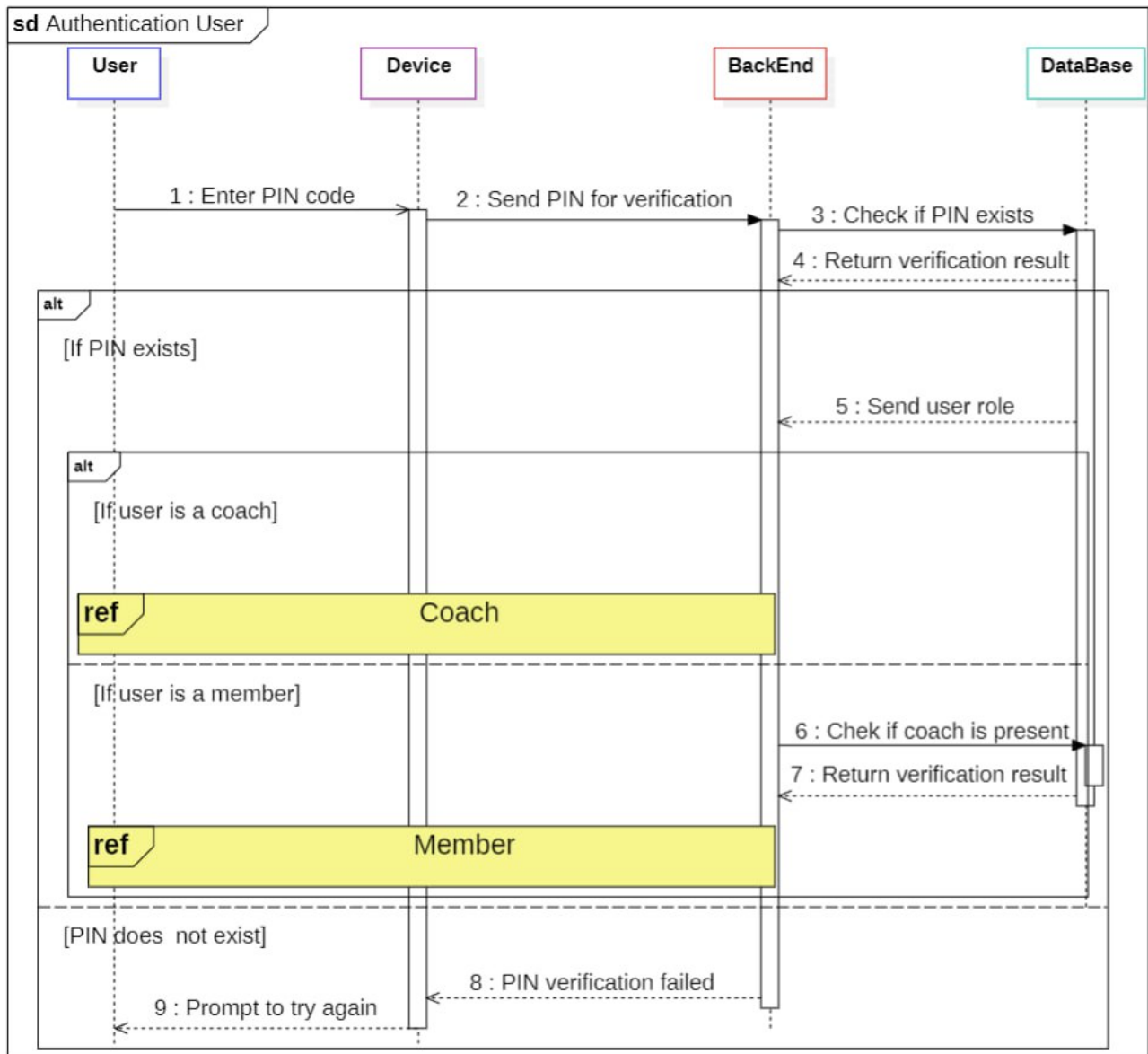


Figure 3.4: Authentication user Sequence Diagram.

### Sequence Diagram of Coach role

The figure 3.5 represents the sequence diagram for the coach role. After the first authentication step is completed, the second phase begins. A voice registration interface is displayed, containing a sentence that is automatically generated by the system after each PIN authentication. The coach reads the displayed sentence clearly and audibly, and the device records the voice for verification.

The system performs a series of operations:

- First, the voice sample is processed.
- Then, the recorded audio is converted into text and compared with the original generated sentence to verify that the spoken phrase matches.
- If the sentence matches, the system proceeds to the voice verification phase, where it extracts the voice features from the input and compares them with those previously stored in the database to determine whether the voice matches the registered coach's identity.
- If the voice verification is successful, the system sends a command to the Arduino microcontroller to unlock the door, granting access.
- If verification fails at either the sentence matching stage or the voice feature comparison stage, the system returns a verification failure message and denies access.

This sequence ensures that access is granted only when both the sentence and the voice identity match the registered data, thereby enhancing the security and reliability of the authentication process.



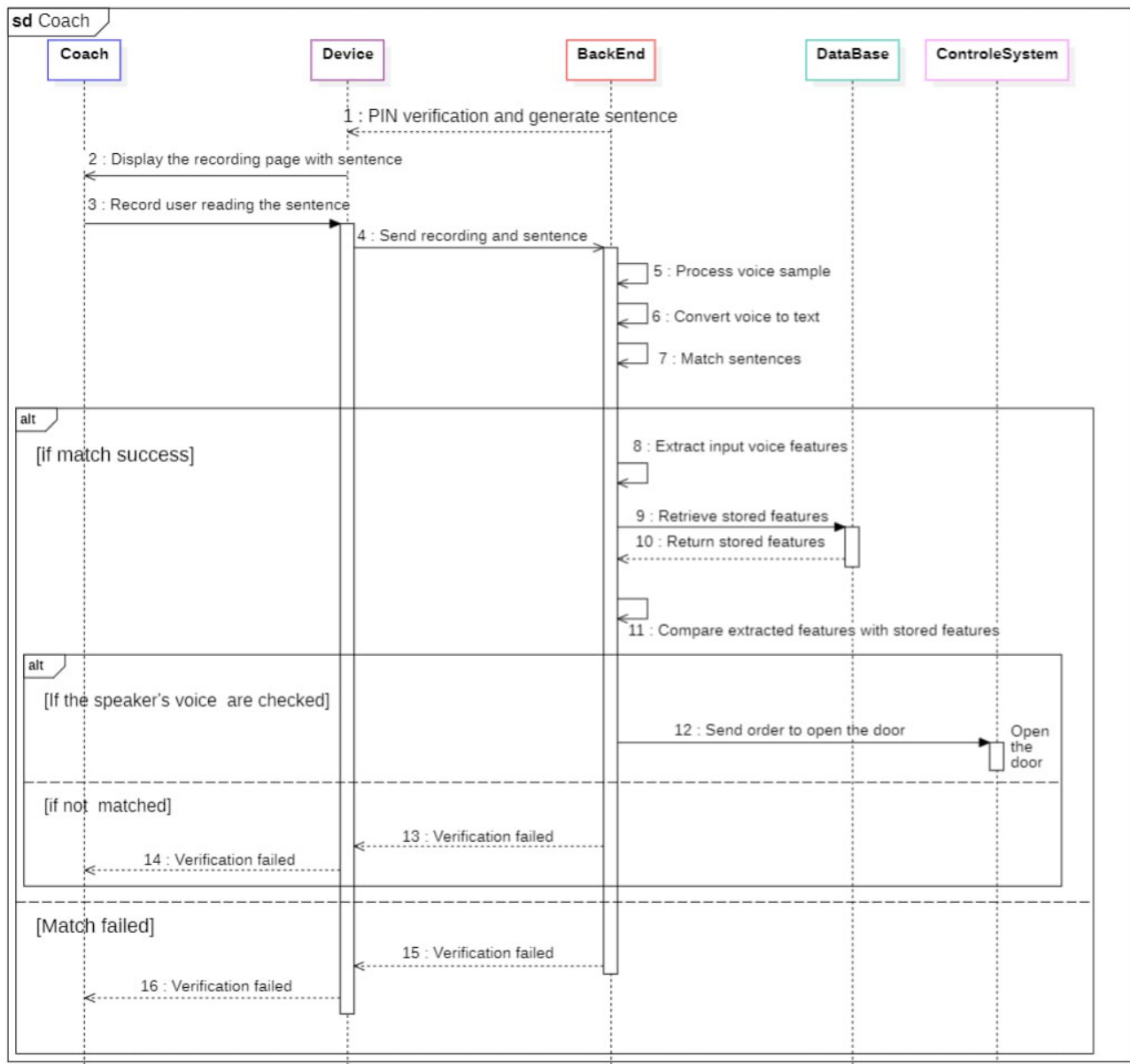


Figure 3.5: Coach role Sequence Diagram.

### Sequence Diagram of Member Role

Figure 3.7 presents the sequence diagram for the Member role. It does not differ significantly from the previous diagram (Figure 3.4). However, it introduces one additional condition: the presence of the swimming coach within the pool.

- If the coach is confirmed to be present in the pool, the member proceeds through the same authentication stages as the coach. Each successful entry results in the deduction of one share from the remaining balance of the member.
- However, if the coach is not present, a notification is displayed to the member indicating that access is denied due to the coach's absence.

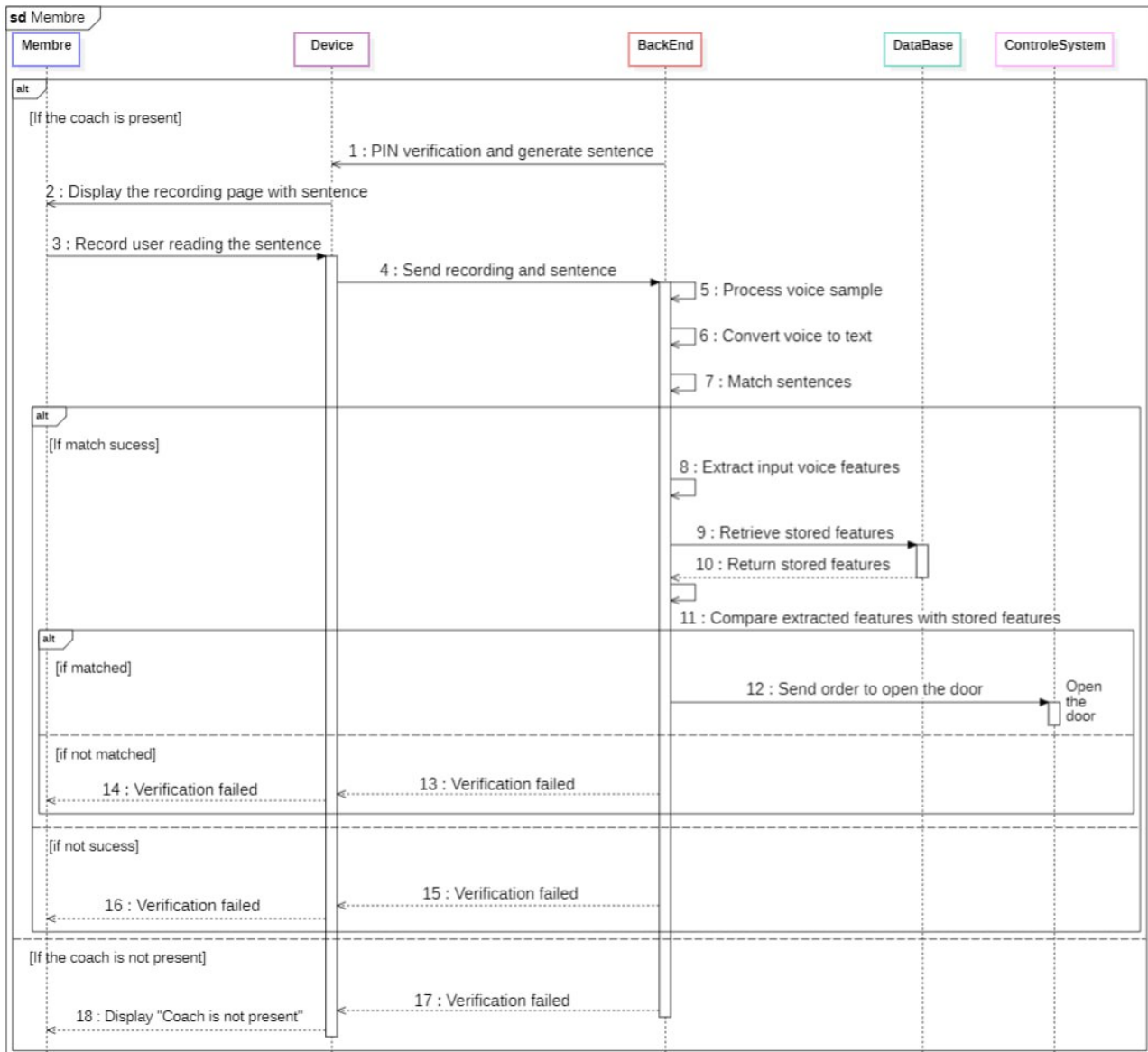


Figure 3.6: Member role Sequence Diagram

### 3.5.2 Flow Chart

The system comprises three primary verification loops. The first loop uses PIN code technology and, as shown in Figure 3.6, it repeats up to three times until the correct code is identified. Once verified, the user proceeds to the second loop, which involves reading a generated sentence. If the user's spoken sentence matches the generated one, the system advances to the final loop.

The third loop employs voiceprint verification, offering unique authentication by confirming that the user's voice matches the stored voiceprint. If successful, the magnetic door switch is activated, granting access. During the same time, the system updates the connected app in real time. Any failed verification attempt triggers an instant notification on the user's device.

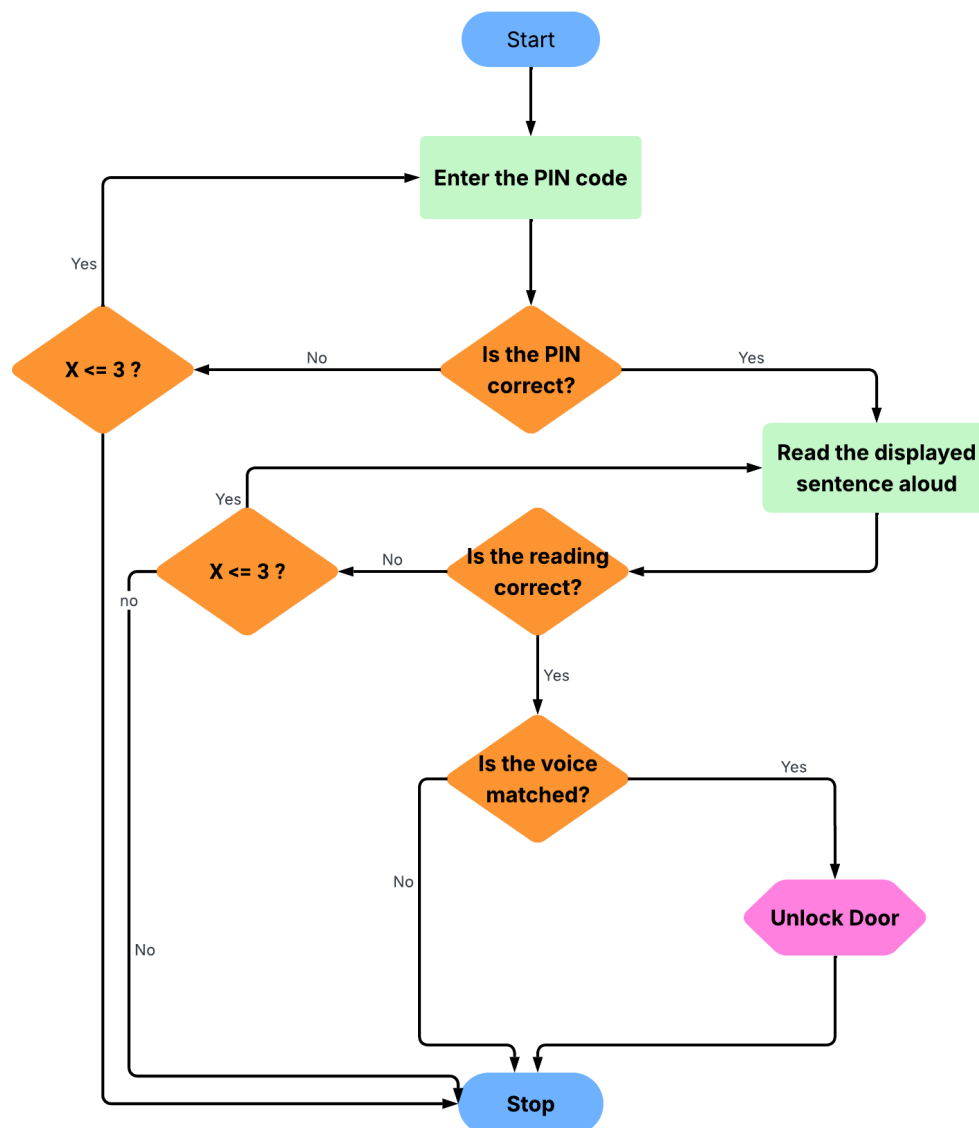


Figure 3.7: Flow Chart Diagram

## 3.6 Conclusion

In this chapter, we presented the conception of our project starting with the problem. Then, we present some UML diagrams that explain more about this project, these diagrams captured the user interactions, system architecture, and dynamic processes in detail. The details of the implementation of the access control verification system will be described in the next chapter.

## **Chapter 4**

### **Implementation and Results**

## 4.1 Introduction

After completing the design of our system, this chapter focuses on the implementation phase. It begins by identifying the essential components, which are categorised into two main groups: software and hardware. This is followed by a description of the steps taken to develop the system. This chapter presents the selected system outputs and application interfaces, highlighting the main features and functionalities.

## 4.2 Development Environment

Our access control system requires both software and hardware components. The software part includes the operating systems, databases, frameworks, and libraries necessary for the front-end and back-end development, while the hardware part comprises the physical components of the system.

### 4.2.1 Software Environment

In this section, the important front-end and back-end tools are described.

- **Visual Studio Code :**

VS Code, short for Visual Studio Code, is a free, open-source code editor developed by Microsoft. It runs on Linux, Windows and macOS. VS Code is designed to make it easier to write web and mobile applications using languages compatible with various development platforms. It comes with built-in support for many programming languages, such as Node.js, JavaScript, HTML, Python, Java, Dart, and more. In this work, we will use it to create a mobile application using the React Native framework[58].

- **Node.js :**

It is a free and open-source JavaScript runtime environment that works across platforms. It enables developers to build servers, web applications, command-line tools, and scripts using JavaScript[59].

- **React Native :**

A JavaScript-based mobile app framework for building natively rendered iOS and Android apps. It allows developers to use the same code base to create applications for different platforms.

- **Expo React Native :**

Expo is a production framework for React Native. It provides development tools that simplify app development, such as file-based routing, a standard library of native modules, and much more. The Expo framework is free and open-source, with an active community on GitHub and Discord. The Expo team works closely with the Meta React Native team to integrate the latest React Native features into the Expo SDK. Expo also offers Expo Application Services (EAS), a set of optional services that complement the Expo framework at every stage of the development process [61].

- **Firebase :**

Firebase is a Backend as a Service (BaaS) platform that was launched in April 2012 and later acquired by Google in 2014 to provide solutions for backend developers. It offers a combination of the key features that work for both web and mobile (Android, IOS) applications, such

as including database management, cloud storage, authentication, cloud messaging, hosting, analytics, remote configuration and more [62].

- **Python Language :**

As defined in [63], Python is a popular interpreted, object-oriented, high-level programming language that is easy to learn and understand. It is suitable for a range of applications, from web development and data analysis to machine learning and automation.

- **Random :**

The Python random module [64] generates pseudorandom numbers, meaning they are not truly random. This module can be used for various random actions, such as generating random numbers and selecting random values from a list or string.

- **Numerical Python (NumPy) :**

Large multidimensional arrays and matrices are supported by NumPy, it is a core package scientific computing in Python, and offers a set of mathematical operations for large arrays. It provides the foundation for numerous other Python scientific and data analysis libraries and is commonly utilised for numerical and array-oriented computing workloads.

- **Torchaudio :**

Torchaudio is a library for audio and signal processing with PyTorch. It provides I/O, signal and data processing functions, datasets, model implementations and application components [65].

- **Noisereducer :**

It is a Python-based noise reduction algorithm designed to reduce noise in time-domain signals such as speech, bioacoustics, and physiological signals. It utilises a technique called "spectral gating," a type of noise gate. The process involves calculating a spectrogram of the signal (and optionally a noise signal) and estimating a noise threshold (or gate) for each frequency band. This threshold is then used to create a mask, which filters out noise below the frequency-dependent threshold[66].

- **Cosine similarity :**

It is a metric used to assess how similar two vectors are within an inner product space. It evaluates the cosine of the angle between the vectors, indicating how closely they align in direction. This method is widely used in text analysis to compare documents based on the occurrence of words or phrases they contain [67].

- **Hypertext Transfer Protocol (HTTP) :**

It is a library which enables an effort to communicate with web services via HTTP requests in flutter. HTTP gives developers the ability to transmit and retrieve data over the internet using an intuitive API for GET, POST, PUT, DELETE, and others. For Flutter apps to integrate network connection, this package is necessary.

- **Arduino IDE :**

Arduino IDE is a software development environment or software application specifically designed for programming any microcontroller board, such as Arduino or NodeMCU. It allows users to write, test, and upload codes in a language which a board understands (i.e. C, C++) and facilitates communication between the computer and the microcontroller board via a USB connection. IDE software includes a set of different programs that are ready to be tested on the device is also comes with built-in libraries that offer additional functionalities for projects. The IDE provides a structured environment to write code[69].

- **SpeechBrain :**

SpeechBrain is a Python-based toolkit developed using PyTorch, designed to support a wide range of speech processing tasks, including speech recognition, speech enhancement, speaker recognition, and other related applications [70]. It offers pre-trained models and a modular framework that allows researchers and developers to quickly build, customise, and deploy state-of-the-art speech systems.

- **FastAPI :**

FastAPI is a modern, high-performance web framework for building APIs and web applications with Python. Introduced in 2018 by Sebastián Ramírez, it stands out from traditional Python frameworks by leveraging advanced features introduced in recent versions of Python 3, such as type hints and asynchronous programming. FastAPI is specifically designed to simplify the development of fast, scalable, and production-ready APIs, while also supporting the creation of traditional web applications. It emphasises clarity, speed, and automatic validation, enabling developers to efficiently handle web requests and responses with minimal boilerplate code. As its name suggests, FastAPI is optimised for speed both in execution and in development workflow [71].

## 4.2.2 Hardware Environment

In this section, we will identify the main hardware components needed to implement our project.

- **Arduino UNO :** The Arduino UNO was used and programmed to control the door's opening after verifying the user's identity through the system. It was also used to receive commands via the Bluetooth HC-05 module and execute them in real-time. More information in chapter 1 [11].

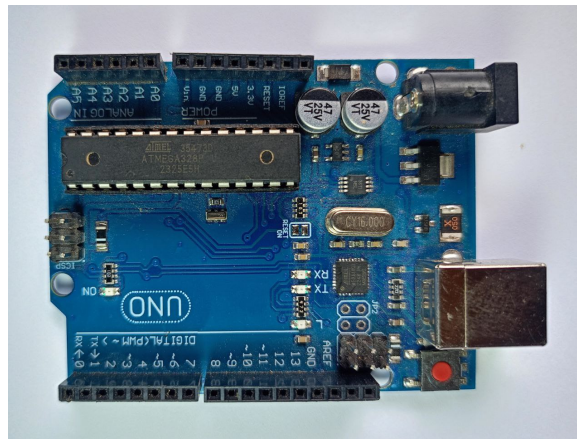


Figure 4.1: Arduino UNO

- **Relay module :** The main purpose of the relay module in our project is to enable us to control the opening of the door when it receives a signal from the microcontroller. More information in Chapter 2 [7].

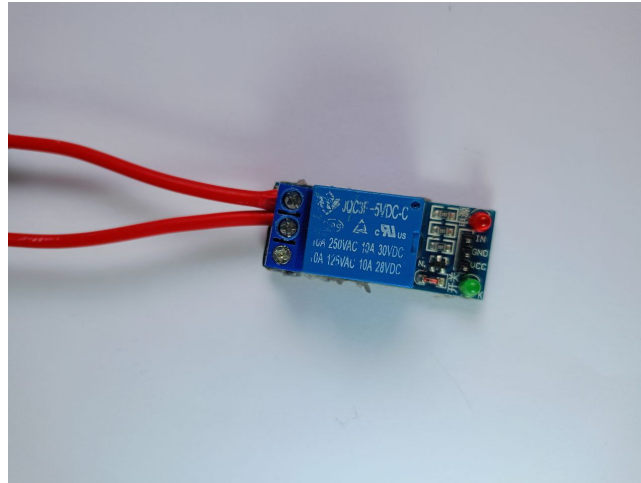


Figure 4.2: Relay Module

- **HC-05 Bluetooth module :** The HC-05 Bluetooth module is a simple and easy-to-use device based on the Serial Port Protocol (SPP), enabling the establishment of a wireless serial connection with ease. In this project, the HC-05 module serves as a wireless bridge between the microcontroller and the mobile app, facilitating seamless serial communication between the two devices.

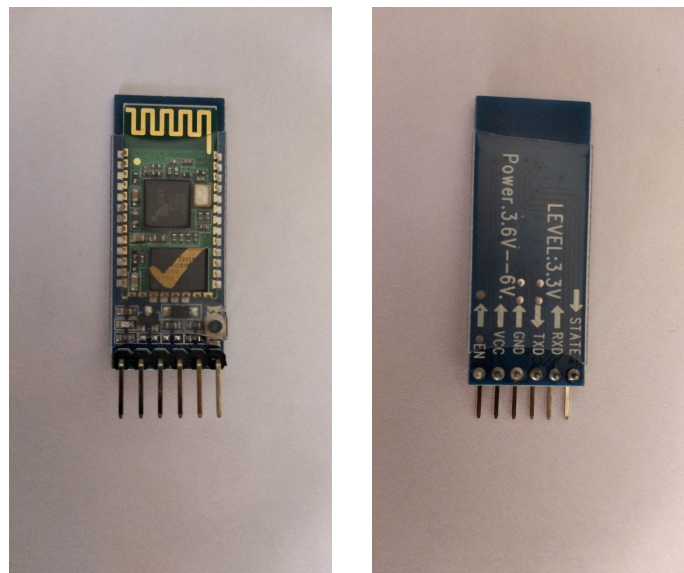


Figure 4.3: Bluetooth Module HC-05



- **Wires :** A wire is a thin, flexible metal strand used to carry mechanical loads, electrical currents, or signals. They are used to establish electrical connections between the various components of the system, including the microcontroller board, the relay module, the battery, and the solenoid lock.

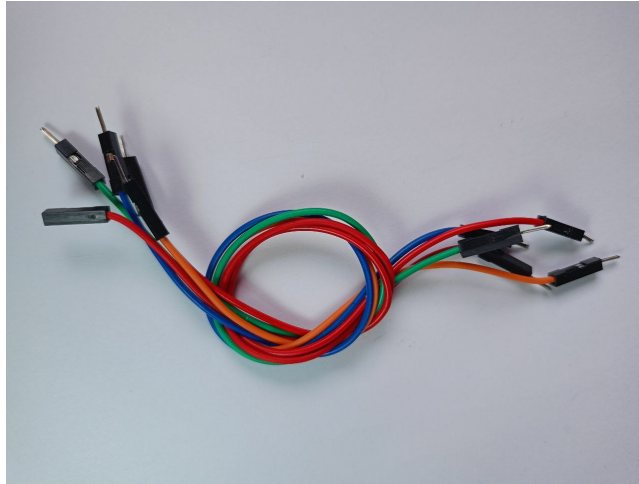


Figure 4.4: Wires

- **Electric lock :** Solenoid electric acts as the locking mechanism in our system. When it receives an electric signal from the relay module, it activates and physically unlocks the door.

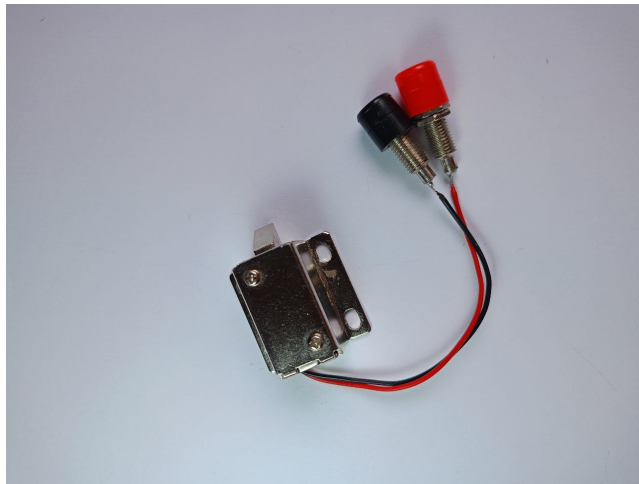


Figure 4.5: Electric lock

- **Battery :** A 12V battery was used to power the electric lock, which is controlled through a relay module connected to the control board.
- **Mobile phone :** Due to the lack of a device designated for display and audio input next to the door, the mobile phone was relied upon as an alternative for both the responsible party and the user party, to test and implement the system in a realistic environment as much as possible.

## 4.3 IA Models Used in the Project

After researching and experimenting on several models to meet the project's requirements in both the voice verification process and generating variable sentences each time (models such as GPT-2, GPT-J, BART, and LLaMA were tested), as well as a model for converting speech to text. And after evaluating performance and efficiency, we decided to rely on these models because they provide us with the required results and achieve the project objectives.

### 4.3.1 ECAPA-TDNN

The ECAPA-TDNN (Emphasised Channel Attention, Propagation and Aggregation in TDNN) model is an advanced neural architecture used for extracting speaker embeddings. It employs a channel- and context-dependent attention mechanism, Multilayer Feature Aggregation (MFA), as well as Squeeze-Excitation (SE) and residual blocks [72]. This design has recently demonstrated impressive performance in the speaker verification domain and has become the most popular model among the TDNN-series, refreshing the state-of-the-art in speaker recognition [73].

Different variants of forensic automatic speaker recognition (FASR) systems based on ECAPA-TDNN have been tested under conditions that simulate real forensic voice comparison scenarios. Using this model as the embedding extraction block, and by applying various normalisation strategies at both embedding and score levels, the system showed strong discriminative power, high accuracy, and precision. These results indicate that ECAPA-TDNN is highly effective as a core component of FASR systems, outperforming previous models under the tested operating conditions [74].

### 4.3.2 Meta-Llama-3-8B-Instruct

Meta-Llama-3-8 B-Instruct is a large and recent language model (LLM) developed by Meta as part of the LLaMA 3 model series. This model is distinguished by its ability to accurately understand and execute instructions, making it suitable for a wide range of applications in natural language processing.

The model was trained on a massive dataset exceeding 15 trillion tokens from publicly available sources, including more than 10 million manually labelled examples. It employs the Transformer architecture with enhancements such as Grouped-Query Attention (GQA) to improve inference efficiency.

The model demonstrates superior performance on several benchmark tests such as MMLU, HumanEval, and GSM-8K, outperforming earlier models like LLaMA 2 and GPT-3.5. It also shows the ability to generalise across multiple tasks, including programming, question answering, and creative writing [76].

### 4.3.3 Whisper

Whisper is an advanced speech model (Automatic Speech Recognition - ASR) developed by OpenAI. The system relies on machine learning techniques to accurately convert spoken speech into written text, supporting multiple languages and offering a variety of interfaces. Whisper is used in applications such as instant translation, conversation transcription, and audio data analysis, making it a powerful tool for translating audio across multiple environments.

## 4.4 Systems Implementation and Interfaces

This section presents the step-by-step system implementation, from user registration and identity verification to sending the unlock command to the Arduino, along with a detailed overview of the application interfaces and user interaction.

### 4.4.1 User Enrollment and Multi-Factor Authentication Workflow

In this section, we explain the most important parts of the code that implements the access control system using artificial intelligence techniques.

#### 1- User Enrollment Process (Audio Processing and Storage)

- Initially, essential libraries are imported, including:
  - torchaudio and numpy for audio processing and numerical operations.
  - SpeakerRecognition from the SpeechBrain library for speaker recognition.
  - Requests to handle HTTP requests, enabling the system to exchange data with the device.
- A pre-trained **ECAPA-TDNN** model is loaded from the SpeechBrain library. This model is specifically designed for speaker verification tasks and was trained on the VoxCeleb dataset to ensure high accuracy.

Listing 4.1: Loading the pre-trained ECAPA-TDNN model

```
# Load the pretrained model for speaker recognition
recognizer = SpeakerRecognition.from_hparams(
    source="speechbrain/spkrec-ecapa-voxceleb",
    savedir="pretrained_models/spkrec-ecapa-voxceleb")
```

- Once the user data is received, a random 4-digit Personal Identification Number (PIN) is generated for the user, as shown in Listing 4.2. This serves as the first factor of authentication.

Listing 4.2: Generating a unique PIN code

```
pin = str(random.randint(1000, 9999))
# Check that the same code does not exist inside Firebase
existing = db.collection("users").where("pinCode", "==",
    int(pin)).get()
```

- After that, raw audio inputs are pre-processed to ensure clean and consistent data for accurate speaker recognition. The preprocessing includes:
  - The audio files are first converted to WAV format using FFmpeg.
  - A noise reduction algorithm is then applied to improve the clarity and quality of the speech signal, making it suitable for further analysis.
- Now, the audio is passed to the **ECAPA-TDNN** model as illustrated in Listing 4.3 to extract a voice embedding a numerical representation capturing unique vocal traits.

Listing 4.3: Extraction of voice embeddings

```
embedding = recognizer.encode_batch(denoised_signal)
return embedding.squeeze(0).squeeze(0).detach().cpu().numpy()
```

These embeddings serve as a voiceprint and form the basis for speaker verification.

- After extracting the audio features from both recordings (each represented as a NumPy array), the arithmetic mean is calculated using the `np.mean(..., axis=0)` function from the NumPy library. This step aims to generate a unified voiceprint that more accurately represents the user's voice than relying on a single recording.
- Finally, all user data (including personal details (e.g., fullName, email, phone, age), number of sessions, role, generated pinCode, and the computed embedding) is stored in Firebase Firestore for future authentication.

## 2- Sentence generation

To generate short and varied sentences each time the user requests access, we implemented the following steps:

- We imported the **GPT4All** library to handle the local AI model, and the **random** library to choose a random topic from the list of selected topics.
- We loaded the **Meta-Llama-3-8B-Instruct** model using the GPT4All interface. This model, developed by Meta, is optimised for local execution on low-resource devices and can generate contextually meaningful and fluent sentences.

Listing 4.4: Loading the pre-trained Meta-Llama-3-8B-Instruct model

```
model = GPT4All("Meta-Llama-3-8B-Instruct.Q4_0.gguf")
```

- After that, we prepared a predefined list of topics that serve as the basis for sentence generation. Each time a new sentence is needed, one topic is randomly selected from this list to ensure diversity and unpredictability in the prompts given to the user.
- Using Python's **random** library, a topic is selected at random, and a request (prompt) is sent to the language model with clear instructions to generate a short sentence of 10 to 15 words. The prompt emphasises the use of simple, easy-to-pronounce vocabulary, while still encouraging creativity and clarity in the generated sentence.

## 3- Authentication and Verification Process

As previously mentioned, the authentication process to open the door involves two sequential stages:

**1- PIN verification :** The user is first prompted to enter a PIN code to verify their identity.

**2- Speaker Verification :** Upon successful PIN entry, the second stage verifies the user's identity by having them repeat a randomly generated sentence. This step is specifically designed to prevent spoofing attempts such as the use of pre-recorded audio by requiring the user to say a new, unpredictable sentence each time.

If the spoken sentence matches the expected one, the process continues to voiceprint verification, which ensures the voice truly belongs to the registered user, providing an additional security layer.

- Initially, the recorded audio undergoes preprocessing: it is converted to .wav format, and a noise reduction algorithm is applied to enhance clarity.

#### Step 1: Transcribe and compare sentences

- The **Whisper** speech-to-text model is loaded to transcribe the user's spoken sentence.

Listing 4.5: Loading Whisper model and Transcribe sentence

```
# Load Whisper model
whisper_model = whisper.load_model("small")
#Use Whisper model to convert audio file to text
def transcribe_audio(audio_path):
    try:
        result = whisper_model.transcribe(audio_path, language="en")
        transcription = result.get('text', '')
        logger.info(f"Transcription successful: {transcription[:500]}")
    return transcription
```

- Both the transcribed and expected sentences are normalised using the **normalize\_text** function to remove differences such as capitalisation, punctuation, and extra spaces. The `difflib.SequenceMatcher` from Python is used to compute the similarity ratio between the two texts, which ranges from 0 (no match) to 1 (exact match).

#### Step 2: Speaker Verification

- First, Audio features (voice embeddings) are extracted from the user's voice using the **ECAPA-TDNN** model. Then, previously stored voice embeddings of registered users are retrieved from the Firebase Firestore database
- Next, using the function **Cosine Similarity**, the similarity between the current voice print and all stored prints is calculated.

Listing 4.6: Matching process

```
similarities=cosine_similarity([query_embedding],stored_embeddings)[0]
best_score = float(np.max(similarities))
best_label = str(labels[best_index])
```

- Final Decision: If the highest similarity score (`best_score`) is greater than or equal to 0.65 (a threshold value selected based on testing and experimentation), the user is recognised, and a confirmation message is shown with the similarity value. If the score is below the threshold, the user is not recognised, and a rejection message is displayed, also indicating the best score found.

## 4.4.2 Mobile Application Development

In the implementation of the mobile application developed using React Native and FastAPI as the backend, the following steps were followed:

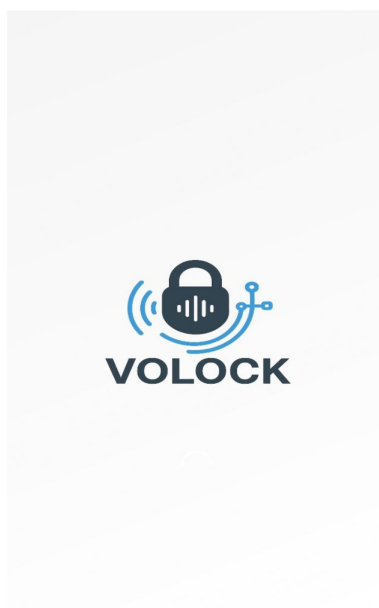
- Utilized the React Native framework with Expo to build a responsive and cross-platform mobile application(Android-iOS).
- Employed FastAPI, a modern Python web framework, as the backend technology to handle server-side logic, including speech processing and text comparison.
- Implemented a modular design structure to ensure code maintainability and clear separation between UI components, logic, and API services.
- Using API requests to send and receive data between the frontend and backend by using JSON as the data transfer format, enabling efficient data transfer and communication.
- Integrated the expo-av library to enable audio recording directly within the mobile application.
- Leveraged Firebase as the database to store and retrieve application data efficiently and reliably.

## 4.4.3 Mobile Application Interfaces

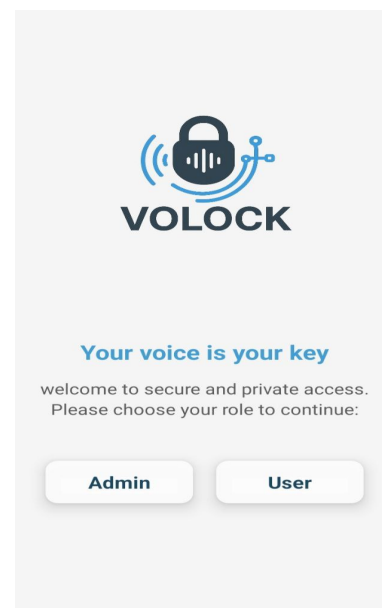
This part provides an overview of our mobile application system, which consists of various interfaces for both facility owners and users. Here, we'll provide an overview of the interfaces for each group.

### 4.3.3.1 Initial Interface and Role-Based Separation

Figure 4.6 presents the application's initial interface, while Figure 4.7 was added to visually separate the administrator interfaces from the user interfaces.



(a) Logo

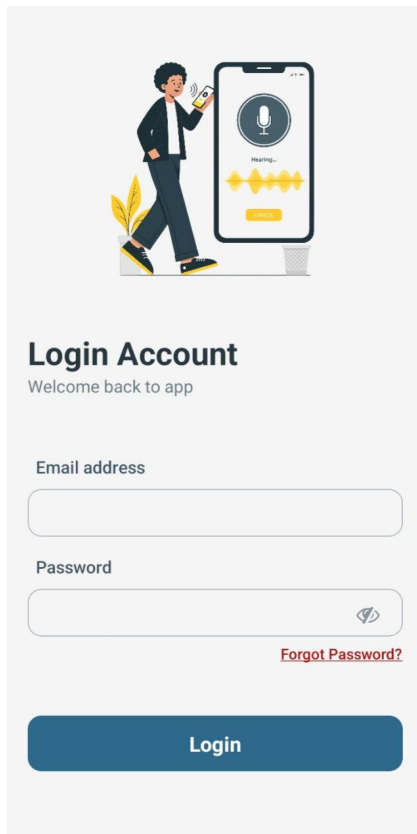


(b) Role page

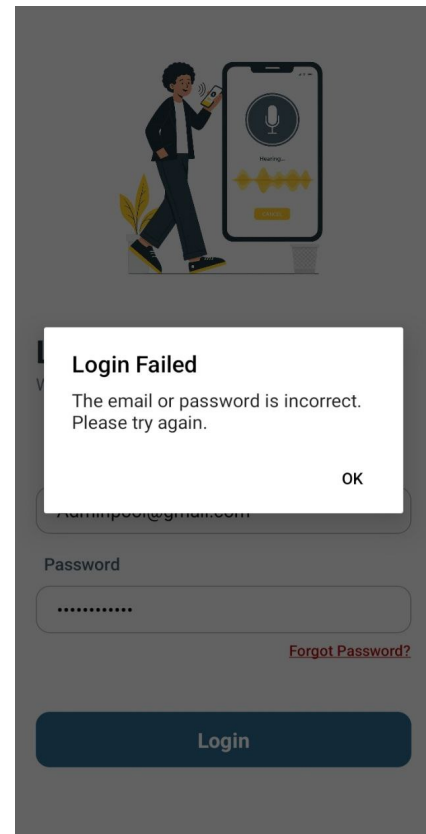
### 4.3.3.1 Admin interfaces

- **Login page**

Figure 4.6 shows the administrator login page for the mobile application, which includes the email and password fields. If the credentials entered are incorrect, an alert message is displayed, as shown in Figure (4.6 b). If the credentials are correct, the administrator is successfully redirected to the new user registration page, as shown in Figure 4.7.



(a) Login page

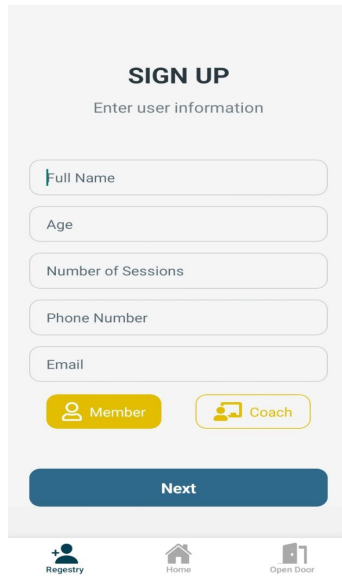


(b) Login page error

Figure 4.6: Login pages

- **Register Page**

Figure 4.7 illustrates the sequence of user interfaces involved in the user registration process. In part (a), the user inputs their personal information. Following this, the user is prompted to record their voice twice, as indicated by the two yellow circles in parts (b) and (c), which serve as visual cues to guide the user through the recording steps. Finally, part (d) confirms the successful completion of the registration process and displays the system-generated PIN code.



**SIGN UP**  
Enter user information

Full Name

Age

Number of Sessions

Phone Number

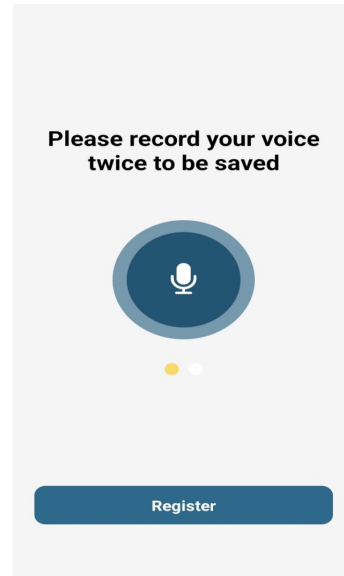
Email

Member Coach

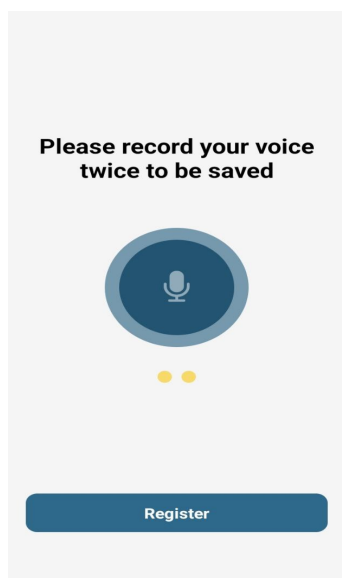
Next

Registry Home Open Door

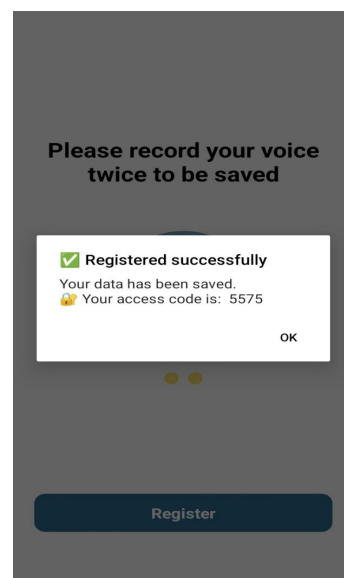
(a) Register page



(b) 1 Voice recording



(c) 2 Voice recording



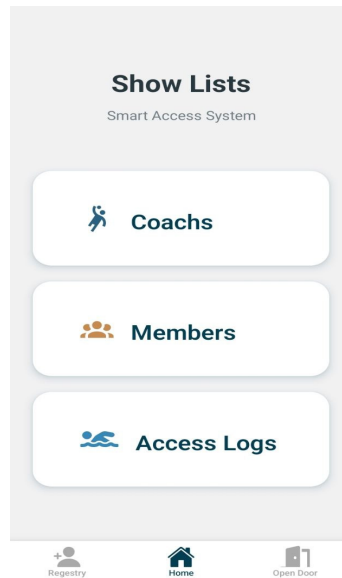
(d) Display PIN code

Figure 4.7: Register pages



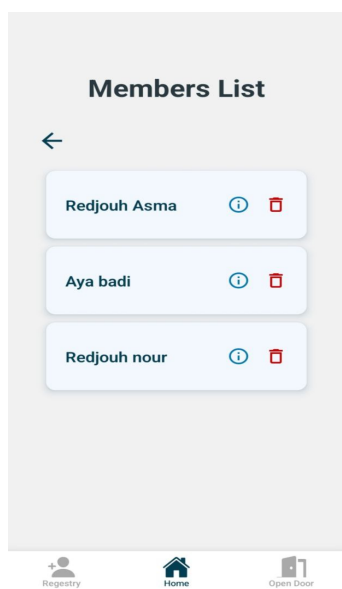
- **User Lists Interface**

After the users have registered on the system, the administrator can access various user lists. Screen (a) provides an overview of the information available to the administrator, including the list of registered members, coaches, and users who have logged in through the portal.

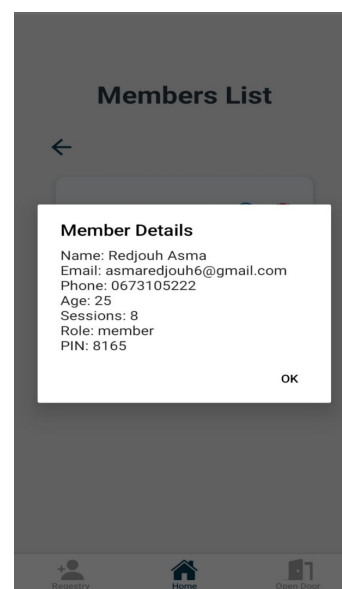


(a) Menu page

This is an example of the menu that appears when the administrator clicks on "Members." From this menu, the administrator can delete a user or view their complete personal information.



(b) Users Accounts



(c) Users Informations

Figure 4.8: User Lists Interface

- **Administrator Door Access**

The administrator, being the highest authority within the system, is granted extensive privileges that exceed those of regular users or trainers. One of these key privileges is the ability to access the system without undergoing the standard verification procedures required of other users, such as entering a PIN code or completing voice authentication. To streamline and simplify the entry process for the administrator, we have implemented a dedicated button within the application. When this button is pressed, it sends a direct command to the system to unlock the door electronically, allowing the administrator to have immediate access to the secured area or facility. This feature has been carefully designed to ensure quick and efficient access, particularly in urgent situations or when administrative intervention is required. It is important to note that the functionality of this button is strictly restricted to users who are registered as administrators in the system, thus maintaining the overall security and integrity of the access control mechanism.

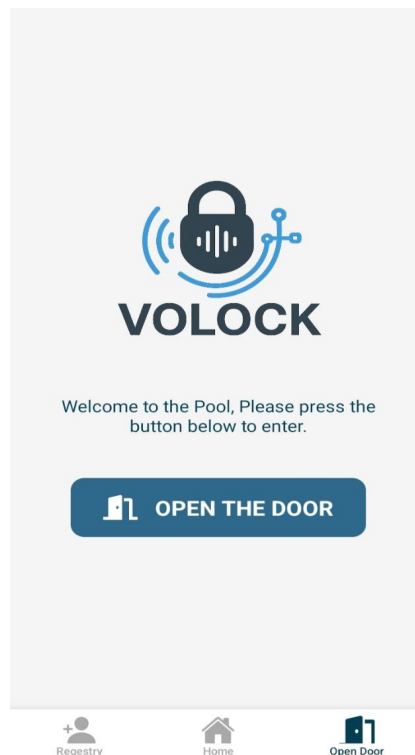


Figure 4.9: Open door page

#### 4.3.3.2 User interfaces

- **Authentication page**

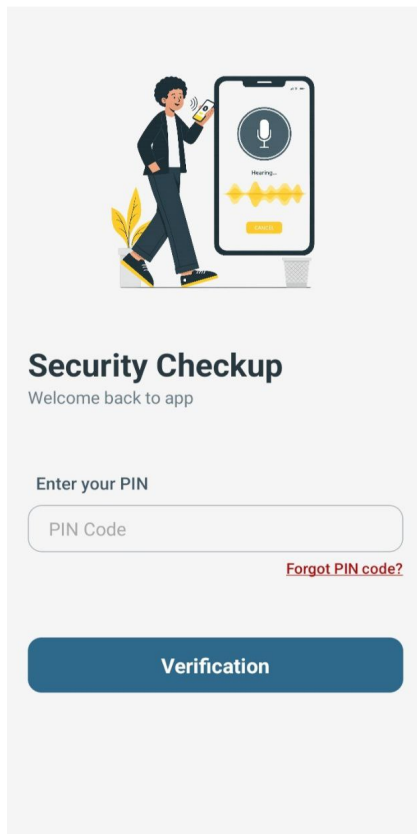
Figure 4.10 illustrates the first user authentication method. In this screen, the user is prompted to enter a four-digit code that was provided during the registration phase. This step serves as a basic security measure to verify the user's identity.

**The user is a coach :**

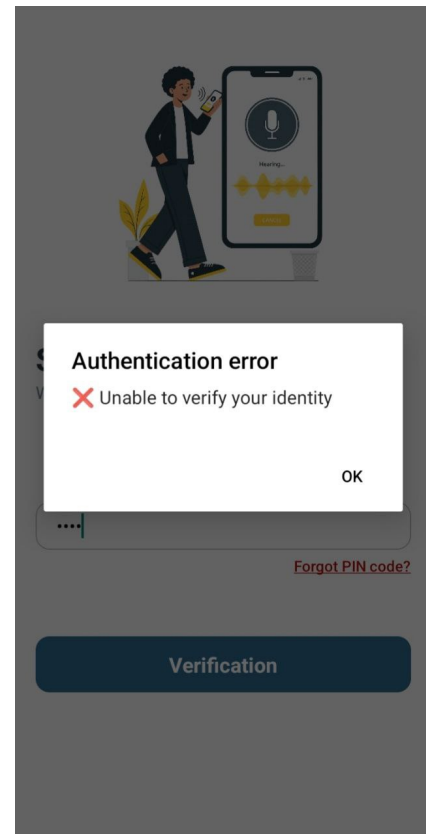
If the code entered is correct, the user is redirected to the main interface (see Figure 4.11). Otherwise, a notification is displayed indicating an incorrect authentication attempt, as shown in Figure 4.10(b).

**The user is a member :**

If the entered code is correct and the coach is logged in, the user is redirected to the main interface (Figure 4.11). If the code is incorrect, a notification is shown (Figure 4.10(b)). However, if the code is correct but the coach is not logged in, a message notifies the member that the coach is currently unavailable.



(a) Login page



(b) Login page error

Figure 4.10: Authentication page

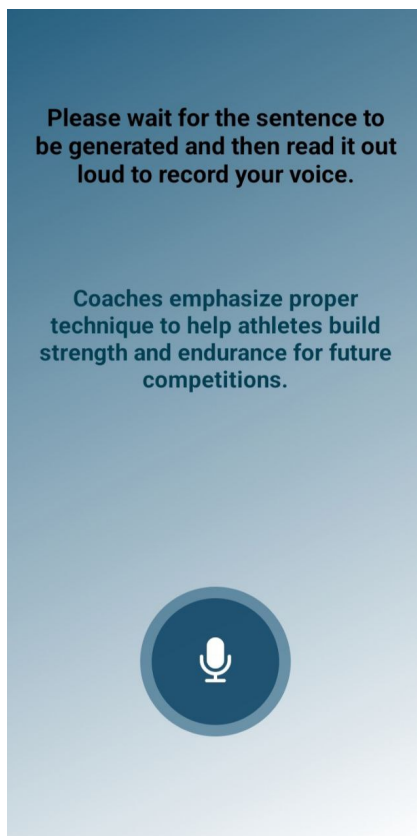
- **Verification page**

After completion of the initial authentication process, the user is presented with the interface shown in Figure 4.11(a).

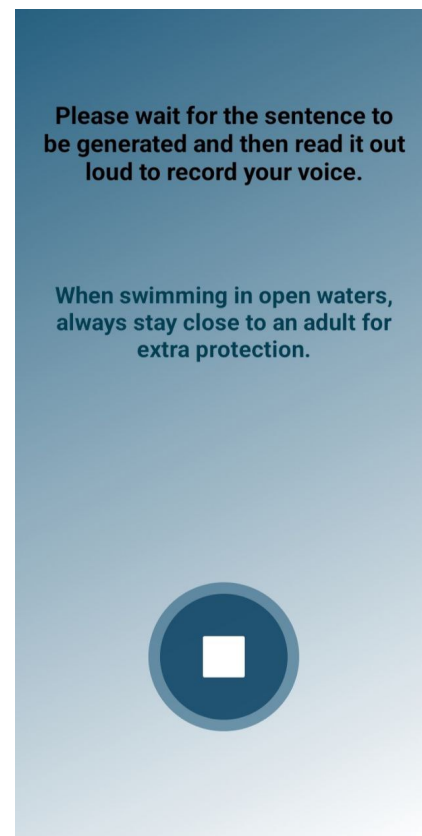
At this stage, a sentence is automatically generated using generative artificial intelligence and displayed to the user. The user is then required to press the microphone icon located at the bottom of the screen and read the sentence displayed aloud. Figure 4.11(b) illustrates the real-time voice recording process. Once the user finishes reading the sentence, they must press the button shown at the bottom of Figure 4.11(b).

The system then proceeds with the verification process as follows:

- If the user reads the sentence correctly and clearly, the system checks whether the user is registered in the database.
  - \* If the user is registered, the door opens automatically and closes after five seconds. The access is logged accordingly.
  - \* If the user is not registered, the door remains closed and no access is granted.
- If the user reads the sentence incorrectly or unclearly, they are allowed up to two additional attempts.
- After three failed attempts, a notification is sent to the system administrator, and access is denied.



(a) Voice Recording Interface



(b) Start Recording Interface

Figure 4.11: Verification page

#### 4.4.4 Electronic Lock Control Integration

The code below illustrates the code of the system (Arduino).

Listing 4.7: Code of System

```
BEGIN

  Initialize Bluetooth serial communication at 9600 baud
  Initialize regular serial monitor at 9600 baud

  Set relay pin as OUTPUT
  Set relay pin to LOW (relay OFF)

  Print "N.O.V.A ready. Waiting for command..."

  LOOP FOREVER:
    IF Bluetooth serial receives data:
      Read incoming string until newline character
      Remove any whitespace from the string
      Print "Received: " followed by the command

      IF command equals "***" OR command equals "ON":
        Turn relay ON
        Print "Relay ON"
        Wait for 5 seconds
        Turn relay OFF
        Print "Relay OFF"

END
```

**The general diagram:** Figure 4.12 shows the hardware wiring diagram.

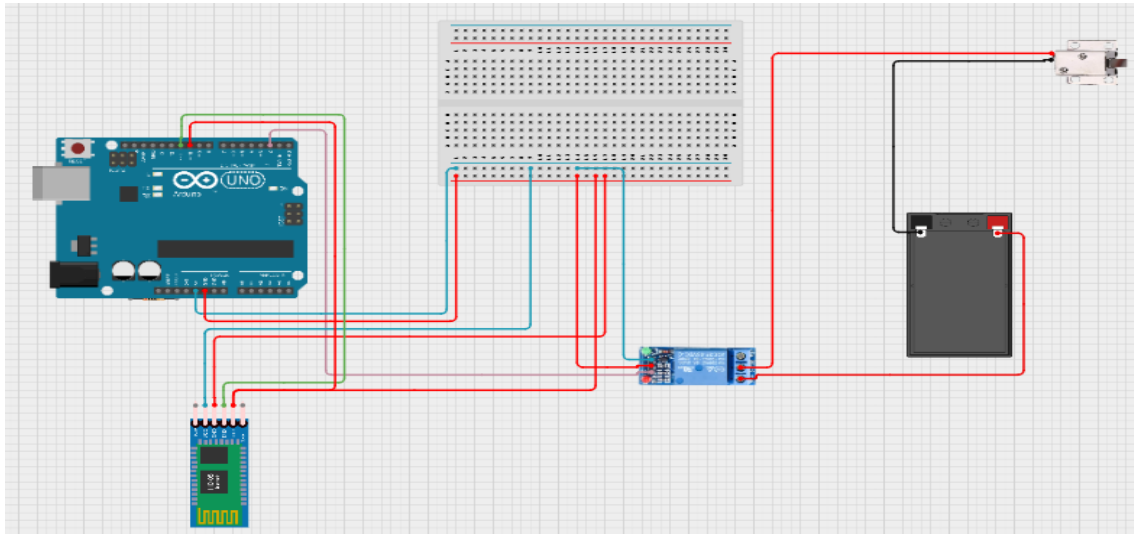


Figure 4.12: Hardware Wiring diagram

**Proposed System Prototype:** The following figures illustrate the prototype and physical setup of the proposed access control system.

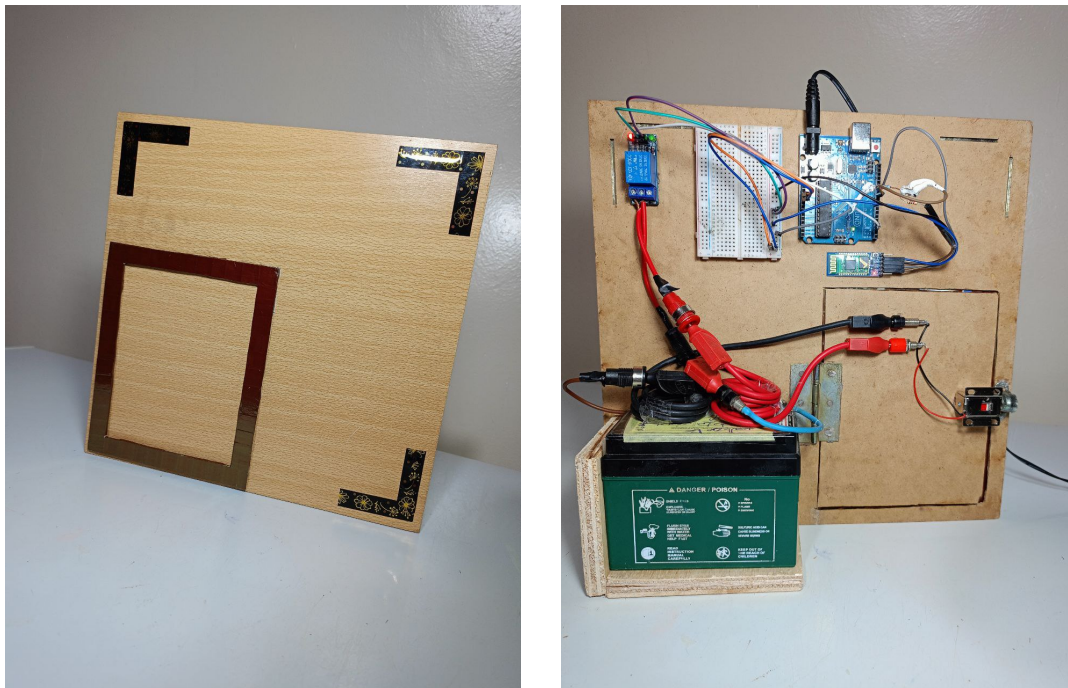


Figure 4.13: Real Picture of Proposed System

## 4.5 Experimentation Examples and Results

Below, we present screenshots from our application, captured during experiments conducted to evaluate the reliability of the system.

### 4.5.1 Experimentation Examples

#### 4.5.1.1 Coach

##### Case 1: Coach recognised and access granted

Figure 4.14 illustrates the successful recognition of the coach. A notification is displayed to confirm access, and the door is opened, as shown in Figure 4.15.

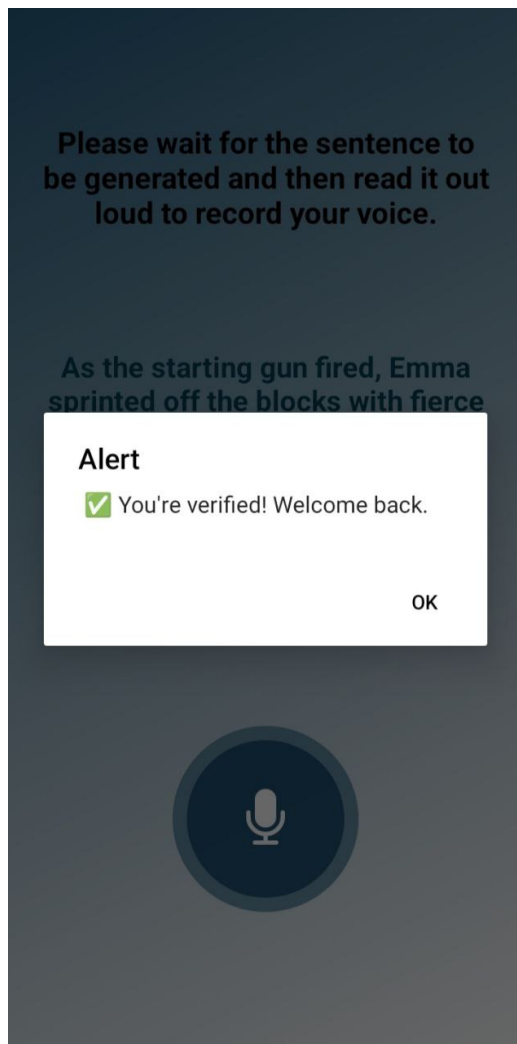


Figure 4.14: User recognised

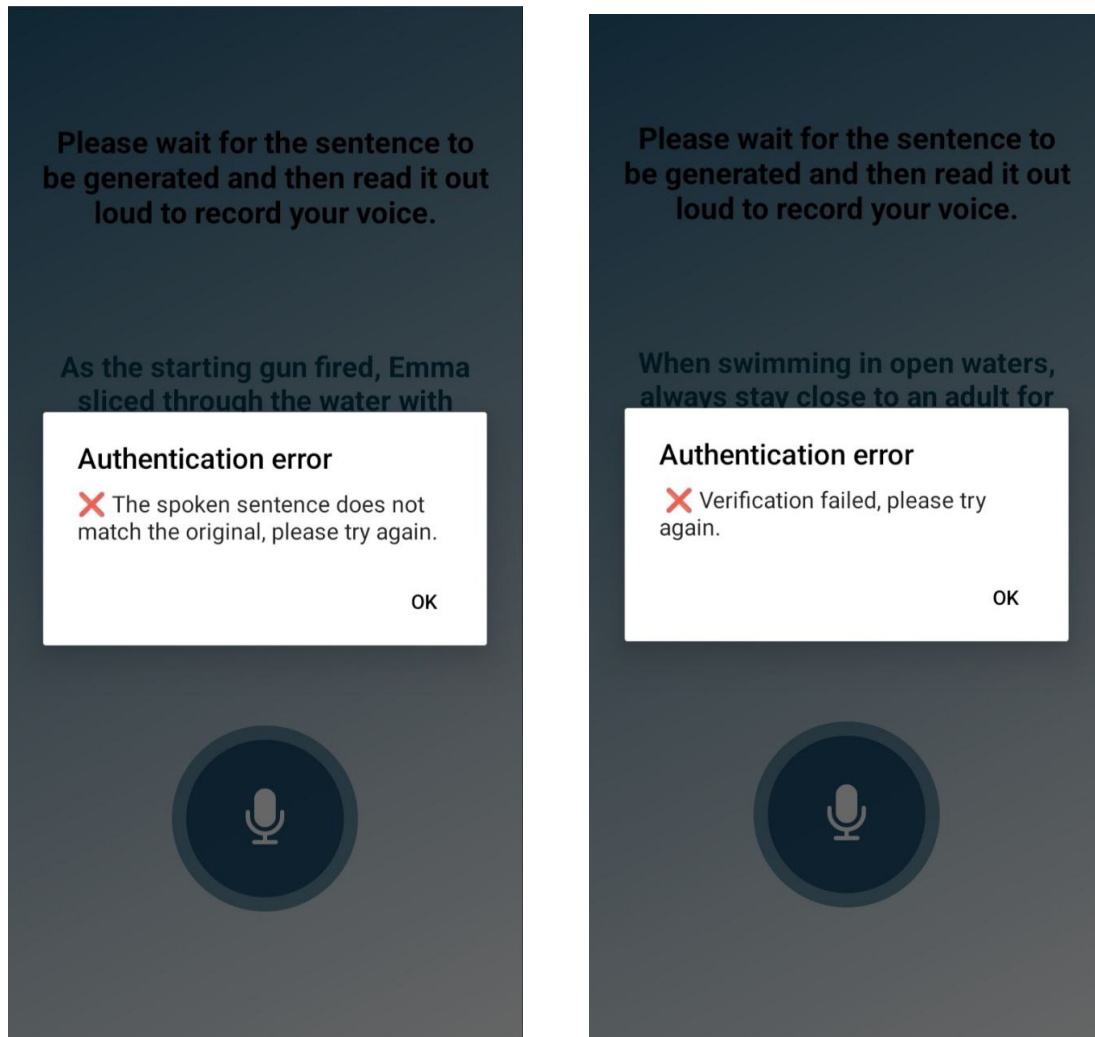


Figure 4.15: Access granted



**Case 2: Coach not recognised and access denied**

Figure 4.16 illustrates a failure to recognise the coach, which may result from either incorrect sentence reading (Figure a) or a voice mismatch (Figure b). As a result, a notification is displayed to inform the coach.



(a) The sentences do not match

(b) Voice recognition failed

Figure 4.16: Coach recognition failed



Figure 4.17 illustrates the failure to recognise the user after three unsuccessful attempts. Consequently, a notification is displayed to inform the user, and the door remains closed, as depicted in Figure 4.18.

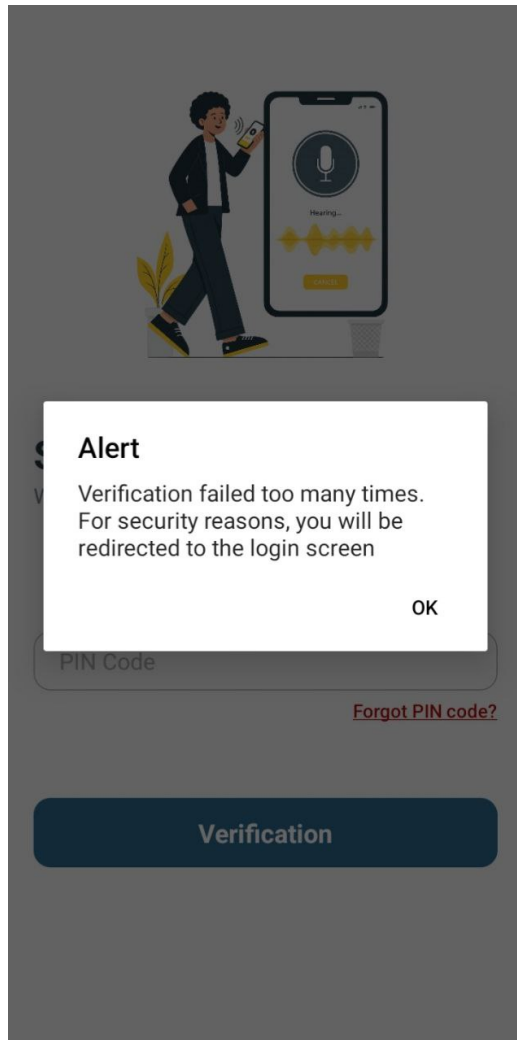


Figure 4.17: User not recognized



Figure 4.18: Access denied

#### 4.5.1.2 Member

##### Case 1: Coach present

In this case, the system first identifies the person as a member. Then it verifies the presence of the coach. If the coach is present, the system proceeds to the second level of authentication, similar to the previous coach scenarios (cases 1 and 2).

**Case 2: Coach not present**

If the coach is not present, the system will block the user from proceeding to the second level of authentication and notify the user that the coach is unavailable.

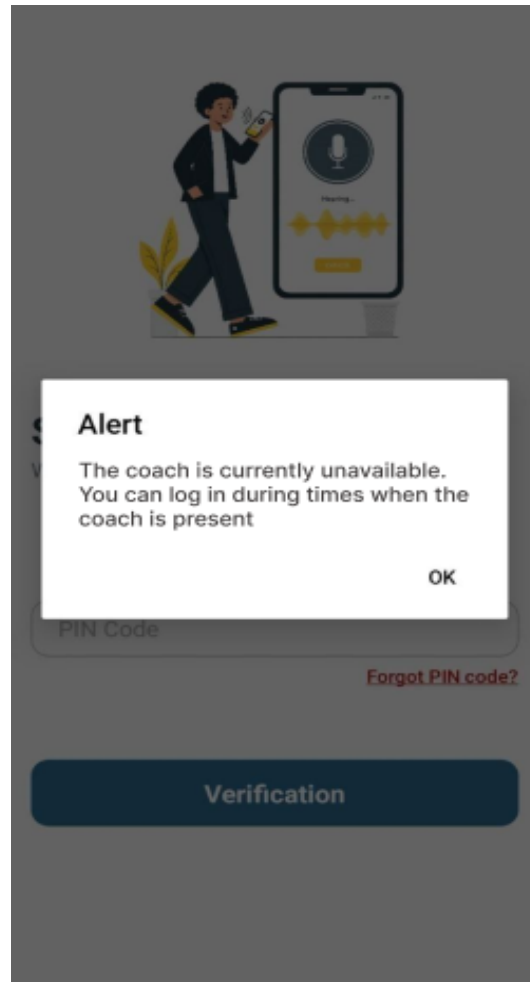


Figure 4.19: Coach not present

### 4.5.2 Some of the sentence-voice matching results

The figures below illustrate the actual results of our system across various test cases. For sentence matching, an acceptance threshold of 0.92 was applied, while for voiceprint matching, a threshold of 0.60 was used. These threshold values were determined through extensive experimentation and performance evaluation to ensure optimal system accuracy.

In the first case, the spoken sentence and the generated sentence matched with 98% similarity, exceeding the sentence matching threshold. As a result, the system proceeded to the second stage of voiceprint verification, where the speaker was successfully verified and identified. The system concluded that the person was authorized to enter.

```
Normalized Transcription: a sturdy fence with a secure gate ensures the safety of your property from unwanted intruders
Normalized Sentence: a sturdy fence with secure gates ensures the safety of your property from unwanted intruders
Similarity: 0.9837837837837838
✓ Proceeding to speaker verification...
✓ Speaker recognized: Redjough abdessatar (Similarity: 0.631)
```

Figure 4.20: Sentence-Voice matching

In this case, although the sentence match was 100%, the person was not identified during the voiceprint verification stage. Therefore, the system concluded that this was an unauthorized entry attempt.

```
Normalized Transcription: when swimming in open waters always stay close to an adult for extra protection
Normalized Sentence: when swimming in open waters always stay close to an adult for extra protection
Similarity: 1.0
✓ Proceeding to speaker verification...
✗ Speaker not recognized (Highest similarity: 0.331)
```

Figure 4.21: Sentence matching and voice mismatch

Finally, the third case represents a mismatch between the two sentences, with a similarity score of 84%, which is below the threshold. Therefore, the system did not proceed to voiceprint verification. The person is allowed to try again two more times.

```
Normalized Transcription: a sturdy fence with the sharp edges can effectively save your property from unwanted intruders
Normalized Sentence: a sturdy fence with sharp edges can effectively safeguard your property from unwanted intruders
Similarity: 0.8469387755102041
✗ The spoken sentence does not match the original.
```

Figure 4.22: Sentence matching and voice mismatch

## 4.6 Conclusion

In this chapter, we presented the practical implementation of our smart access control system highlighting the integration of cutting-edge IA models such as ECAPA-TDNN for speaker verification, Meta-Llama-3-8B-Instruct for generating sentences, and Whisper for speech-to-text conversion. We detailed the development environment, both software and hardware, and demonstrated the structure and workflow of the mobile application and its interaction with the electronic lock mechanism. Furthermore, through a series of experiments, we validated the functionality and efficiency of the proposed system.

# General conclusion

Access control systems are among the fundamental pillars of the security infrastructure in modern facilities, especially with the growing need for smart and secure solutions that keep pace with the developments of the digital age. From this perspective, this project presents an innovative approach that integrates the Arduino unit, a low-cost and flexible electronic controller with artificial intelligence technologies, including generative AI, to build an effective and smart access control system.

The work began with a comprehensive study of the theoretical and technical framework, covering key concepts of access control systems, their classifications, and the weaknesses of traditional solutions. Several related previous works were also analysed, along with the exploration of how IoT and AI technologies can enhance these systems.

Based on these foundations, we designed and developed an integrated system that provides dual-factor authentication, relying on a secret code generated at the time of registration and a unique voiceprint verified through a randomly generated sentence at each access attempt. This increases system security and makes imitation more difficult. Advanced AI models were integrated into the system, such as ECAPA-TDNN for speaker verification, Whisper for speech-to-text conversion, and Meta-Llama-3-8B-Instruct for dynamic sentence generation.

A smartphone application was developed for the administrator to manage the registration of authorised users and generate secret codes. Meanwhile, the end user interacts with a smart device installed next to the door, where a sentence is displayed and read aloud by the user. The system then verifies the match between the spoken sentence and the original one, followed by voiceprint verification. Upon successful authentication, a command is sent to the Arduino unit via the Bluetooth module to unlock the door. This division of roles reflects a true integration between software and hardware components, enhancing the system's security and efficiency in real-life scenarios.

Initial testing conducted with a group of users demonstrated the system's effectiveness in terms of authentication accuracy and security level, despite some challenges related to pronunciation or environmental noise. Nevertheless, the obtained results are encouraging and open the door for future enhancements, such as adding other verification methods like facial recognition or location-based authentication. Overall, this project can be considered a first step toward developing smart, low-cost, and secure access systems that combine technical simplicity with the advanced capabilities of artificial intelligence, making it suitable for application in educational institutions, laboratories, or even smart homes.

## **Limitation**

- The sentence generation model requires significant computing resources, particularly a GPU. As a result, when run on our computer using only a CPU, we observed a noticeable delay in sentence generation.
- Loud environmental noise may hinder the accuracy of the speech recognition process.
- The application interface is currently available in only one language, which may limit accessibility for non-native speakers.

## **Prospects for improvement and Future Work**

As we strive to continuously evolve and improve our application, we have identified several key areas for future development that aim to enhance both user experience and system functionality. The proposed enhancements include:

- To ensure service continuity at minimal cost and improve system reliability in real-world environments without requiring investment in dedicated physical servers or keeping a computer permanently active, we propose deploying Python code on a free cloud hosting platform such as Replit or Render. Alternatively, a Raspberry Pi device can be used as a low-power smart server capable of running the application continuously and stably within a local network or over the Internet.
- Integrate a module to detect fake or manipulated audio input, thereby enhancing the security and integrity of the system.
- Implement a mechanism that automatically generates a new sentence every 5 seconds if the current sentence has not been read by the user, maintaining engagement and real-time interaction.
- Provide multilingual interface options to enhance usability for all users.

# Bibliography

- [1] J. Emms, "A definition of an access control systems language," *Comput. Stand. Interfaces*, vol. 6, no. 4, pp. 443--454, 1987.
- [2] A. Kukreti, "Access control and authentication for secure systems and networks," *NeuroQuantology*, vol. 20, no. 5, pp. 5321--5329, 2022.
- [3] MCA COMPANIES, "Access Control Systems" [Online]. Available: <https://callmc.com/security-solutions/access-control-systems>. Accessed: Mar. 3, 2025.
- [4] CDVI, "What is Access Control?" [Online]. Available: <https://www.cdvi.fr/en/what-is-access-control/>. Accessed: Jun. 5, 2025.
- [5] V. C. Hu, D. F. Ferraiolo, and D. R. Kuhn, "Assessment of access control systems," *NIST Interagency Report 7316*, 2006.
- [6] A. Masoumzadeh, H. van der Laan, and A. Dercksen, "BlueSky: Physical access control—characteristics, challenges, and research opportunities," in *Proc. 27th ACM Symp. Access Control Models Technol. (SACMAT)*, 2022, pp. 163--172.
- [7] E. B. Fernandez, J. Ballesteros, A. C. Desouza-Doucet, and M. M. Larrondo-Petrie, "Security patterns for physical access control systems," in *Data and Applications Security XXI: 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, USA, July 8-11, 2007, Proceedings*, Springer, 2007, pp. 259--274.
- [8] M. Boroš and F. Lenko, "Importance of electronic access control systems and the need for their testing," in *Proc. Int. Conf. Diagnostics Electr. Eng. (Diagnosticska)*, Sept. 2020, pp. 1--4.
- [9] NPSA, "Control and Use of Key Locks" [Online]. Available: <https://www.npsa.gov.uk/system/files/documents/npsa-control-and-use-of-key-locks.pdf>. Accessed: Apr. 1, 2025.
- [10] US Patent 3,774,424 A, "Access control system," issued Nov. 27, 1973. [Online]. Available: <https://patents.google.com/patent/US3774424A/en>. Accessed: Apr. 25, 2025.
- [11] N. Zakaria, A. Tria, and N. Igelouzene, "Étude et réalisation d'une carte de commande de contrôle d'accès à base d'Arduino," *Projet de fin de cycle*, Département d'Électronique, Université Mohamed El-Bachir El-Ibrahimi, Bordj Bou Arreridj, Algérie, 2025.
- [12] K. Rana and S. Kathirvel, "Unsung heroes in managing COVID-19 pandemic in India: The changed role of security guards in hospitals," *Int. J. Health Syst. Implement. Res.*, vol. 4, no. 1, pp. 5--10, 2020.

- [13] S. Sudahnan, "Kewenangan satpam sebagai tenaga keamanan di perusahaan," *Perspektif*, vol. 16, no. 3, pp. 140--148, 2011.
- [14] X. Zhu, S. K. Mukhopadhyay, and H. Kurata, "A review of RFID technology and its managerial applications in different industries," *J. Eng. Technol. Manag.*, vol. 29, no. 1, pp. 152--167, 2012.
- [15] ASIARFID, "What is RFID?" [Online]. Available: <https://www.asiarfid.com/what-is-rfid.html>. Accessed: May 4, 2025.
- [16] BSIA, "Biometrics Authentication Technique" [Online]. Available: [https://www.bsia.co.uk/zappfiles/bsia-front/pdf2024/181\\_biometrics\\_authentication.pdf](https://www.bsia.co.uk/zappfiles/bsia-front/pdf2024/181_biometrics_authentication.pdf). Accessed: May 2, 2025.
- [17] N. Singla, M. Kaur, and S. Sofat, "Automated latent fingerprint identification system: A review," *Forensic Sci. Int.*, vol. 309, pp. 110--187, 2020.
- [18] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. London: Springer, 2009.
- [19] P. Komarinski, *Automated Fingerprint Identification Systems (AFIS)*. Amsterdam, The Netherlands: Elsevier, 2005.
- [20] D. Valdes-Ramirez, M. A. Medina-Pérez, R. Monroy, O. Loyola-González, J. Rodríguez-Ruiz, A. Morales, and F. Herrera, "A review of fingerprint feature representations and their applications for latent fingerprint identification: Trends and evaluation," *IEEE Access*, vol. 7, no. 1, pp. 48484--48499, 2019.
- [21] L. Li, X. Mu, S. Li, and H. Peng, "A review of face recognition technology," *IEEE Access*, vol. 8, pp. 139110--139120, 2020.
- [22] I. Pattnaik, A. Dev, and A. K. Mohapatra, "A face recognition taxonomy and review framework towards dimensionality, modality and feature quality," *Engineering Applications of Artificial Intelligence*, vol. 126, p. 107056, 2023.
- [23] A. Murhula, "Conception et mise en place d'une plateforme de sécurisation par synthèse et reconnaissance biométrique de documents de trafic," *Projet de fin d'études*, Polytechnique INITELEMATIQUE BURUNDI, Ingénieur Civil en Informatique et Télécommunications, 2015.
- [24] H. Fathee and S. Sahmoud, "Iris segmentation in uncooperative and unconstrained environments: state-of-the-art, datasets and future research directions," *Digital Signal Processing*, vol. 118, pp. 103--244, 2021.
- [25] H. Biswas, V. Sarkar, P. Sen, and D. Sarddar, "Smart city development: Theft handling of public vehicles using image analysis and cloud network," in *Recent Trends in Computational Intelligence Enabled Research*, Academic Press, 2021, pp. 155--169.
- [26] J. Billa, "Speech recognition," in *Wiley Encyclopedia of Telecommunications*, 2003.
- [27] L. Lamel and J.-L. Gauvain, "Speech recognition," in *The Oxford Handbook of Computational Linguistics*, Oxford University Press, 2012, pp. 305--322.
- [28] K. R. Alluri and A. K. Vuppala, "A study on the emotional state of a speaker in voice bio-metrics," in *Advances in Ubiquitous Computing*, Academic Press, 2020, pp. 223--236.



- [29] K. Balasubramanian, V. Karthik, and V. K. Padmanaban, "Smart multi verification based security system," *El-Cezeri*, vol. 10, no. 2, pp. 193--207, 2020.
- [30] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787--2805, 2010.
- [31] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645--1660, 2013.
- [32] Arduino, "LCD Displays," [Online]. Available: <https://docs.arduino.cc/learn/electronics/lcd-displays/>. Accessed: Jun. 5, 2025.
- [33] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, 2023.
- [34] M. N. Mowla, N. Mowla, A. S. Shah, K. M. Rabie, and T. Shongwe, "Internet of Things and wireless sensor networks for smart agriculture applications: A survey," *IEEE Access*, vol. 11, pp. 145813--145852, 2023.
- [35] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22--32, 2014.
- [36] H. M. Rai, A.-U. Rehman, A. Pal, S. Mishra, and K. K. Shukla, "Use of Internet of Things in the context of execution of smart city applications: a review," *Discover Internet of Things*, May 2023.
- [37] J. J. P. C. Rodrigues, D. B. R. Segundo, H. A. Junqueira, M. H. Sabino, R. M. Prince, J. Al-Muhtadi, and V. H. C. de Albuquerque, "Enabling technologies for the Internet of Health Things," *IEEE Access*, vol. 6, pp. 13129--13141, 2018.
- [38] P. Chakravarthy, K. Thamizhoviya, S. Kavitha, and S. Meena, "Design of NFC reader for enhancement of mobile payments," *Int. J. Smart Sens. Intell. Syst.*, vol. 10, pp. 186--198, 2017.
- [39] Z. Wang and Z. Wang, "A survey on security and privacy in emerging sensors and IoT systems," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 2, pp. 1041--1079, 2017.
- [40] C. Cheng and X. Jing, "A survey of proximity sensors," *Sensors and Actuators A: Physical*, vol. 233, pp. 48--62, 2015.
- [41] S. Umchid, V. Sutthipibul, A. Vorapantrakool, P. Vipattipumiprates, and T. Wangkham, "Development of voice controlled wheelchair for persons with physical disabilities," in *Proc. 9th Int. Conf. Autom., Control Robot. Eng. (CACRE)*, Jul. 2024, pp. 112--116.
- [42] ElectroGlobal, "Voice recognition module speech recognition module V3," [Online]. Available: <http://electroglobal.in/product/voice-recognition-module-speech-recognition-module-v3/>. Accessed: May 4, 2025.
- [43] V. Vujović and M. Maksimović, "Raspberry Pi as a Sensor Web node for home automation," *Computers and Electrical Engineering*, vol. 44, pp. 153--171, 2015.

- [44] VEEROBOT, "Infrared Proximity Obstacle Detecting Sensor Module," [Online]. Available: <https://www.amazon.in/VEEROBOT-Infrared-Proximity-Obstacle-Detecting/dp/B0115NCT4U>. Accessed: May 4, 2025.
- [45] J. Yun and S.-S. Lee, "Human Movement Detection and Identification Using Pyroelectric Infrared Sensors," *Sensors*, vol. 14, no. 5, pp. 8057-8081, 2014.
- [46] S. Katta, S. Ramatenki, and H. Sammeta, "Smart irrigation and crop security in agriculture using IoT," in *AI, Edge and IoT-Based Smart Agriculture*, Academic Press, 2022, pp. 143--155.
- [47] OMCHSMP, "What is a proximity sensor?" [Online]. Available: <https://www.omchsmpls.com/what-is-a-proximity-sensor/>. Accessed: May 4, 2025.
- [48] P. Nag, A. Sharma, and P. Tripathi, "Smart door lock system: Enhancing home security using Bluetooth technology," *International Journal of Computer Applications*, vol. 116, no. 11, pp. 23-27, 2014.
- [49] S. Janpla, C. Jewpanich, N. Tachpetpaiboon, W. Prongsanthia, and B. Jewpanich, "The development of smart flowerpot based on Internet of Things and mobile and web application technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, pp. 423--433, Apr. 2022.
- [50] Parteek, "A review paper on IoT advantages and disadvantages," *International Journal of Research and Analytical Reviews (IJRAR)*, vol. 6, no. 2, pp. 444--448, 2019. [Online]. Available: [http://ijrar.com/upload\\_issue/ijrar\\_issue\\_20544386.pdf](http://ijrar.com/upload_issue/ijrar_issue_20544386.pdf)
- [51] A. Agarwal, N. Hada, D. Virmani, and T. Gupta, "A novel design approach for smart door locking and home security using IoT," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 6, no. 8, Aug. 2017. [Online]. Available: <http://www.ijirset.com>
- [52] N. Bakshi and V. Prabhu, "Face recognition system for access control using principal component analysis," in *Proc. 2017 Int. Conf. on Intelligent Communication and Computational Techniques (ICCT)*, pp. 145--150, Dec. 2017.
- [53] A. C. R. Aldawiraa, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door security system for home monitoring based on ESP32," *Procedia Computer Science*, vol. 157, pp. 673--682, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S187705091931187X>
- [54] M. M. Yilwatda, J. A. Enokela, and N. Y. Goshwe, "Implementation of a two-level security door access using keypad and voice recognition," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 6, no. 9, pp. 1--6, Sep. 2017.
- [55] N. Shome, A. Sarkar, A. K. Ghosh, R. H. Laskar, and R. Kashyap, "Speaker recognition through deep learning techniques: A comprehensive review and research challenges," *Periodica Polytechnica Electrical Engineering and Computer Science*, vol. 67, no. 3, pp. 300--336, 2023, doi: 10.3311/PPee.20971.
- [56] D. J. Morerwa, P. Owolawi, and G. Aiyetoro, "Examination hall entry control system using RFID," in *2020 IEEE Int. Conf. on Communication, Networks and Satellite (COMNETSAT)*, pp. 1--6, 2020, doi: 10.1109/COMNETSAT50251.2020.9328923.

- [57] "What is Unified Modeling Language (UML)?," [Online]. Available: <https://www.visualparadigm.com/guide/uml-unified-modeling-language/what-is-uml/>. Accessed: May 3, 2025.
- [58] A. Del Sole, *Visual Studio Code Distilled: Evolved Code Editing for Windows, macOS, and Linux*, 2019, pp. 1--3. [Online]. Available: [http://repo.darmajaya.ac.id/5039/1/Visual%20Studio%20Code%20Distilled\\_%20Evolved%20Code%20Editing%20for%20Windows%2C%20macOS%2C%20and%20Linux%20%28%20PDFDrive%20%29.pdf](http://repo.darmajaya.ac.id/5039/1/Visual%20Studio%20Code%20Distilled_%20Evolved%20Code%20Editing%20for%20Windows%2C%20macOS%2C%20and%20Linux%20%28%20PDFDrive%20%29.pdf). Accessed: Apr. 26, 2025.
- [59] Node.js, "Node.js," [Online]. Available: <https://nodejs.org/en>. Accessed: May 1, 2025.
- [60] Mozilla, "JavaScript documentation," [Online]. Available: <https://developer.mozilla.org/fr/docs/Web/JavaScript>. Accessed: May 1, 2025.
- [61] React Native, "Environment Setup," 2025. [Online]. Available: <https://reactnative.dev/docs/environment-setup>. Accessed: May 1, 2025.
- [62] M. H. B. Tram, "FIREBASE," B.Sc. thesis, 2019, p. 10. [Online]. Available: [https://www.theseus.fi/bitstream/handle/10024/263641/Mai\\_Tram.pdf?sequence=2](https://www.theseus.fi/bitstream/handle/10024/263641/Mai_Tram.pdf?sequence=2). Accessed: Apr. 26, 2025.
- [63] Python Software Foundation, "What is Python? Executive Summary," 2023. [Online]. Available: <https://www.python.org/doc/essays/blurb/>. Accessed: Apr. 26, 2025.
- [64] GeeksforGeeks, "Python random module," 2024. [Online]. Available: <https://www.geeksforgeeks.org/python-random-module/>. Accessed: Apr. 25, 2025.
- [65] PyTorch, "PyTorch Audio," 2023. [Online]. Available: <https://pytorch.org/audio/stable/index.html>. Accessed: Apr. 25, 2025.
- [66] PyPI, "Noisereduce," 2024. [Online]. Available: <https://pypi.org/project/noisereduce/#:~:text=Noisereduce%20is%20a%20noise%20reduction,a%20form%20of%20Noise%20Gate>. Accessed: Apr. 25, 2025.
- [67] J. Han, M. Kamber, and J. Pei, "Getting to know your data," in *Data Mining*, 3rd ed., Amsterdam, Netherlands: Elsevier, 2012, pp. 39--82.
- [68] Ngrok, "Ngrok platform," 2024. [Online]. Available: <https://ngrok.com/>. Accessed: Apr. 26, 2025.
- [69] N. Dangi, "Monitoring environmental parameters: Humidity and temperature using Arduino-based microcontroller and sensors," Thesis, 2017, p. 8. [Online]. Available: [https://www.theseus.fi/bitstream/handle/10024/142235/Dangi\\_Nagendra.pdf](https://www.theseus.fi/bitstream/handle/10024/142235/Dangi_Nagendra.pdf)
- [70] D. Borra, F. Paissan, and M. Ravanelli, "SpeechBrain-MOABB: An open-source Python library for benchmarking deep neural networks applied to EEG signals," *Computers in Biology and Medicine*, vol. 182, p. 109097, 2024.
- [71] F. Voron, *Building Data Science Applications with FastAPI: Develop, manage, and deploy efficient machine learning applications with Python*. Birmingham, UK: Packt Publishing, 2023.

- [72] B. Desplanques, J. Thienpondt, and K. Demuynck, "ECAPA-TDNN: Emphasized Channel Attention, Propagation and Aggregation in TDNN Based Speaker Verification," in *Proc. Interspeech*, 2020, pp. 3830--3834.
- [73] C. Haitao, L. Yu, and Y. Yun, "Research on voiceprint recognition system based on ECAPA-TDNN-GRU architecture," in *Proc. 2023 IEEE 2nd Int. Conf. on Electrical Engineering, Big Data and Algorithms (EEBDA)*, Nanjing, China, Feb. 2023, pp. 1508--1513.
- [74] F. Sigona and M. Grimaldi, "Validation of an ECAPA-TDNN system for forensic automatic speaker recognition under case work conditions," *Speech Communication*, vol. 158, p. 103045, 2024.
- [75] A. Grattafiori, A. Dubey, A. Jauhri, A. Pandey, A. Kadian, A. Al-Dahle, A. Letman, A. Mathur, A. Schelten, A. Vaughan, and A. Yang, "The llama 3 herd of models," \*arXiv preprint arXiv:2407.21783\*, Jul. 2024.
- [76] A. Grattafiori et al., "The llama 3 herd of models," *arXiv preprint arXiv:2407.21783*, Jul. 2024.