

Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique



Université de Ghardaïa



Faculté des Sciences et Technologies
Département de Automatique et électromécanique

L'incubateur d'entreprises de l'Université de Ghardaïa

Mémoire présenté en vue de l'obtention du diplôme de

MASTER

Domaine : Sciences et Technologies

Filière : Automatique

Spécialité : automatique et système

Mémoire de fin d'études pour l'obtention du diplôme de Master
en Automatique et Systèmes, dans le cadre de l'arrêté ministériel
1275 – Diplôme de fin d'études – Startup / Brevet d'invention

Thème

**Intelligent System for Access Control and Management in the
Laboratories of the Faculty of Science and Technology**

Soutenu publiquement le : 25/06/2025

**Par : ABISMAIL MOHAMMED
BOUROUROU OMAR**

Devant : MOSBAH CHARAF ABDELKARIM

Année universitaire 2024/2025

Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique
Université de Ghardaïa



Faculté des Sciences et Technologies
Département de Automatique et électromécanique

Mémoire présenté en vue de l'obtention du diplôme de

MASTER

Domaine : Sciences et Technologies

Filière : Automatique

Spécialité : automatique et système

Par : ABISMAIL MOHAMMED
BOUROUROU OMAR

Thème

**Intelligent System for Access Control and Management in the
Laboratories of the Faculty of Science and Technology**

Soutenu publiquement le : 25/06/2025

Devant le jury :

AISSA REBAI	MAB	Univ. Ghardaïa	Président
RAFIK EULDJI	MAB	Univ. Ghardaïa	Examineur
ABDELMADJID TIMMAOUI	PR	Representative of the Incubator	Examineur
SALAH BOUHOUN	URAER	Representative of the Economic Partner	Examineur
MOSBAH CHARAF ABDELKARIM	MCB	Univ. Ghardaïa	Supervisor
BEKKAR BELGACEM	MCA	Univ. Ghardaïa	Co-supervisor

Contents

Acknowledgment	v
Abstract	vi
List of Figures	vi
List of Tables	viii
General Introduction	2
1 Access Control Systems (ACS)	4
1.1 introduction	4
1.1.1 Definition and Concept	4
1.2 Evolution in History	5
1.3 General Purposes of Access Control Systems	6
1.3.1 Security & Defense	7
1.3.2 Organization & Productivity	7
1.3.3 Auditing & Accountability	8
1.3.4 Integration & Scalability	8
1.4 The Importance of Access Management in Sensitive Environments (Laboratories as a Model)	8
1.4.1 Protecting Valuable Resources and Assets	9
1.4.2 Ensuring Occupational Safety	9
1.4.3 Protecting Intellectual Property and Data Confidentiality	10
1.4.4 Effective Organization and Event Tracking	10
1.4.5 Challenges and Unique Requirements for Laboratories	10
1.5 Modern Technologies in Smart Access Management Systems	11
1.5.1 The Concept of a "Smart System"	11
1.5.2 The Role of Central Web Servers	12
1.5.3 Web Applications	12
1.5.4 Internet of Things (IoT) in Access Management	12
1.5.5 Biometric Authentication Technologies	13
1.5.6 Additional Verification Methods	13
1.6 Conclusion	14
2 Project Motivation and Problem Statement	15
2.1 Introduction	15
2.2 Current Situation Analysis in the College of Science and Technology, Challenges and Costs	16

2.2.1	Human Resource Allocation for Access Control and Security	16
2.2.2	Financial Analysis of Current Costs	16
2.2.3	Administrative and Operational Challenges	19
2.3	Problem Statement	19
2.3.1	Reasons for Selecting the Solution	20
2.4	Orientation Toward the Proposed Solution	21
2.4.1	Centralized Management and Real-Time Operations	21
2.4.2	Automated Monitoring and Intelligent Analytics	21
2.4.3	Scalability and Future-Proofing	22
2.4.4	Implementation Strategy and Change Management	22
2.5	Conclusion	22
3	Hardware Design for Secure Access Control	23
3.1	Introduction	23
3.2	System Components	23
3.2.1	ESP32 Development Board	24
3.2.2	Fingerprint Reader Module	26
3.2.3	Understanding and Operation of a 3x4 Matrix Keypad	28
3.2.4	Relay Module	33
3.2.5	Buzzer	36
3.2.6	Power Supply Design	38
3.3	System Schematic	39
3.3.1	Circuit Schematic and Component Analysis	41
3.4	Dual Authentication System Code	42
3.5	Conclusion	43
4	Software Design for Secure Access Control	44
4.1	Introduction	44
4.2	Programming the ESP32 Unit	45
4.2.1	Operating Mechanism	48
4.3	Back-end System	49
4.3.1	Flask Framework	49
4.3.2	User Management and Authentication (Flask-Login)	49
4.3.3	Database (SQLAlchemy)	50
4.4	Frontend (User Interface)	51
4.4.1	Administrative Dashboard (<code>index23.html</code>):	51
4.4.2	Login Page (<code>login.html</code>)	53
4.4.3	Flash Messages (<code>index23.css</code>)	54
4.5	Conclusion	55
	General Conclusion	56
	Bibliography	58

Acknowledgment

First and foremost, we express our profound gratitude to Allah, the Most Merciful, for granting us the strength, patience, and determination to accomplish this humble work. We would like to extend our sincere thanks to our supervisor, Dr. Mosbah Charaf Abdelkarim, for his trust, continuous support, and insightful guidance, which were essential to the success of this project. We are also especially grateful to our co-supervisor, Dr. Belgacem BEKKAR, for his valuable guidance, availability, and constructive feedback.

We are deeply thankful to the members of the review committee for their interest and for enriching our work with their valuable suggestions. Moreover, we thank all the professors who have guided us throughout our academic journey, sharing their knowledge and supporting us along the way.

Finally, we acknowledge all those who, directly or indirectly, played a part in the completion of this work.

ملخص:

يهدف هذا العمل إلى تطوير نظام ذكي ومتكامل للتحكم الآمن في الوصول إلى المختبرات والمراقبة عن بعد. يتناول المشروع تحديات الأمان والكفاءة في أنظمة الوصول التقليدية من خلال اقتراح حل يجمع بين أجهزة التحكم المادية الذكية (مثل ي SP32 وقارئات بصمات الأصابع) وتطبيق ويب مركزي للإدارة والمراقبة. يوفر النظام آلية مصادقة مرنة، ويسجل بدقة جميع محاولات الدخول والخروج، ويسمح للمسؤولين بالتحكم الشامل في الأذونات والإشراف عن بعد على الأنشطة، مما يعزز أمان المختبرات ويسهل إدارتها.

الكلمات المفتاحية:

نظام التحكم الذكي في الوصول، إنترنت الأشياء، إدارة المختبرات، بصمة الإصبع، لوحة مفاتيح رقمية، المراقبة عن بعد، نظام تسجيل الدخول، أمان المختبر، واجهة برمجة التطبيقات، تتبع الوصول.

Abstract:

This project presents the design and implementation of an intelligent and integrated system for secure laboratory access control and remote monitoring. It addresses the challenges of security and efficiency found in traditional access methods by providing a practical solution that combines smart physical control devices—such as ESP32 microcontrollers and fingerprint readers—with a centralized web application for management and supervision. The system offers a flexible authentication mechanism, accurately logs all access attempts, and enables administrators to manage permissions and monitor activities remotely. By doing so, it significantly enhances laboratory security and simplifies overall facility management.

Keywords:

Intelligent Access Control System, Internet of Things (IoT), ESP32, Flask, Laboratory Management, Fingerprint, Digital Keypad, Remote Monitoring, Login System, Laboratory Security, SQLAlchemy, RESTful API, Tailwind CSS, Access Tracking.

Résumé:

Ce projet présente la conception et la mise en œuvre d'un système intelligent et intégré pour le contrôle d'accès sécurisé aux laboratoires ainsi que la surveillance à distance. Il répond aux défis de sécurité et d'efficacité posés par les méthodes d'accès traditionnelles en proposant une solution pratique qui combine des dispositifs de contrôle physiques intelligents — tels que les microcontrôleurs ESP32 et les lecteurs d'empreintes digitales — avec une application web centralisée pour la gestion et la supervision. Le système offre un mécanisme d'authentification flexible, enregistre avec précision toutes les tentatives d'accès, et permet aux administrateurs de gérer les autorisations et de surveiller les activités à distance. Il contribue ainsi à renforcer la sécurité des laboratoires tout en facilitant leur gestion.

Mots-clés: Système intelligent de contrôle d'accès, Internet des objets (IoT), ESP32, Flask, Gestion de laboratoire, Empreinte digitale, Clavier numérique, Surveillance à distance, Système de connexion, Sécurité des laboratoires, SQLAlchemy, API RESTful, Tailwind CSS, Suivi d'accès.

List of Figures

1.1	Evolution Access Control	5
1.2	Mecanic Key	5
1.3	Magnetic Card	6
1.4	Smart Cards	6
1.5	Biometric System	7
1.6	Cloud Access	7
1.7	Components access control	8
1.8	Risks Laborator	9
1.9	Before/After access control	11
1.10	Biometric Process	14
2.1	Faculty of Science and Technology	16
2.2	Organizational Chart of the Faculty of Science and Technology	18
3.1	esp32 board	24
3.2	ESP32 WROOM 32E Pinout Diagram	25
3.3	AS608 Fingerprint Reader Module	26
3.4	AS608 Fingerprint Module Pinout Diagram	27
3.5	Wiring diagram of the AS608 fingerprint module connected to the ESP32	27
3.6	4x3Keypad Module	29
3.7	4x3 Keypad Arrangement	30
3.8	4x3 Membrane Keypad Pinout	31
3.9	4x3 Membrane Keypad Wiring	32
3.10	Relay Module	33
3.11	Single Relay Module	33
3.12	Output Relay Module	34
3.13	Indicator Relay Module	34
3.14	relay module pinout	35
3.15	Wiring Relay Module to ESP32	35
3.16	door lock	36
3.17	Buzzer	37
3.18	Buzzer Wiring to ESP32	38
3.19	charger 12V	38
3.20	LM7805	39
3.21	Complete System Hardware Schematic	40
3.22	Organigram of Access Control System	42
4.1	Diagram of Connection Softwares	45
4.2	Flowchart of the ESP32 Authentication and Access Control Process	46

4.3	Diagram Back End Server	49
4.4	User Management With Features	52
4.5	Laboratory Management With Features	52
4.6	Access Log Control	53
4.7	Admin Login Page	54

List of Tables

2.1	Monthly and Annual Costs of Access Control Staff (in Dinar)	17
3.1	Pin connections between AS608 and ESP32	28
3.2	4x3 Matrix Keypad Pin Connections to ESP32	32

General Introduction

Laboratories in academic institutions, particularly those within the Faculty of Science and Technology, often contain sensitive equipment, hazardous materials, and confidential data. Ensuring secure, reliable, and efficient access to these facilities is therefore of paramount importance. Traditional access control systems (ACS), such as mechanical locks or standalone digital keypads, present numerous limitations in terms of flexibility, scalability, auditability, and centralized management.

In recent years, advances in embedded systems and web technologies have opened the door for the development of intelligent, integrated access solutions. These systems leverage the Internet of Things (IoT), biometric authentication, and real-time data communication to provide enhanced functionality, user experience, and administrative control.

This work aims to design and implement an intelligent system for access control and management in the laboratories of the Faculty of Science and Technology. The system integrates smart hardware components, including microcontrollers (ESP32), fingerprint sensors, and digital keypads, with a centralized web-based application built using `Flask` and modern web technologies. The solution provides multi-factor authentication, secure access logging, and remote monitoring capabilities to meet the security and usability demands of a modern laboratory environment.

The thesis is organized into four main chapters:

- **Chapter 1: Access Control Systems (ACS)**

This chapter presents an overview of traditional and modern access control systems, their components, technologies, and limitations, as well as the evolution towards intelligent and networked solutions.

- **Chapter 2: Project Motivation and Problem Statement**

This chapter outlines the practical motivations that led to this work, highlights the shortcomings of existing systems, and defines the core problem addressed by the proposed solution.

- **Chapter 3: Hardware Design for Secure Access Control**

This chapter details the architecture and implementation of the physical hardware components, including sensors, controllers, actuators, and their integration to form the embedded layer of the system.

- **Chapter 4: Software Design for Secure Access Control**

This chapter focuses on the development of the system's software infrastructure, covering both the embedded firmware and the backend/frontend components of the web application for real-time management and monitoring.

By combining robust hardware with an intuitive software interface, this project contributes to the development of modern, intelligent access systems tailored for academic laboratory environments. The

proposed system not only enhances security but also simplifies administrative tasks through real-time data access, remote control, and detailed activity logging.

Chapter 1

Access Control Systems (ACS)

1.1 introduction

Access Control Systems (ACS) represent a fundamental cornerstone in modern security paradigms, serving as critical mechanisms for safeguarding assets, information, and personnel across a diverse spectrum of environments [1]. More than mere gatekeepers, these sophisticated systems constitute comprehensive frameworks comprising interconnected hardware and software components, meticulously engineered to regulate and monitor the flow of individuals and resources within defined perimeters [2]. Their primary objective is to enforce security policies by precisely determining who is authorized to enter a given physical or logical space, under what conditions (e.g., specific times or dates), and to what extent they can interact with or utilize the resources therein.

The scope of ACS extends far beyond simple door-locking mechanisms. They are intricate ecosystems designed to manage and enforce access permissions, ensuring that only authenticated and authorized entities can gain entry or perform specific actions. This encompasses both physical security—controlling access to buildings, rooms, or restricted areas—and logical security—governing access to computer systems, networks, and sensitive data. In essence, ACS are indispensable tools for maintaining order, preventing unauthorized intrusion, ensuring regulatory compliance, and providing accountability within any controlled environment. Their evolution, driven by advancements in digital technologies and biometrics, continues to enhance their precision, reliability, and adaptability to complex security demands.

1.1.1 Definition and Concept

Access Control Systems (ACS) are security solutions designed to enforce predefined policies that regulate access rights to physical and logical assets. Broadly defined, they are integrated systems that control access to resources—whether physical spaces such as doors, rooms, buildings, and restricted zones, or logical assets such as data, networks, and computer systems—based on a set of rules established in advance. The core objective of these systems is to manage access along three fundamental axes:

- **Identity (Who):** Verification of the subject or entity attempting to access.
- **Time (When):** Defining permitted access times (e.g., office hours, holidays).
- **Location/Authority (Where/What):** Establishing the areas that are available or the processes that can be performed.

These systems rely on authentication to authenticate the user's identity and authorization to grant the correct permissions.

1.2 Evolution in History

Access control systems developed tremendously over the decades Figure 1.1, adapting to developments in technology and expanding security needs [3] :

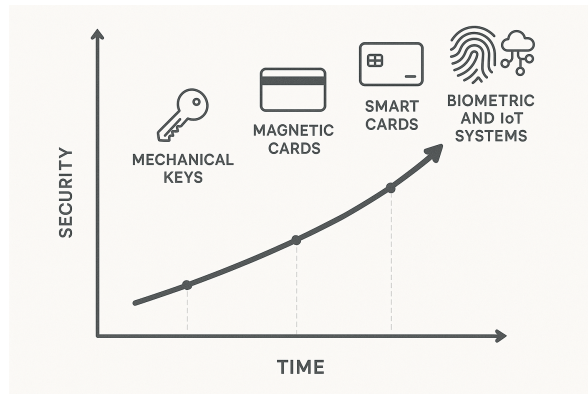


Figure 1.1: Evolution Access Control

- **Mechanical Conventional Keys:** The very first access control technique, where access depends on the possession of a physical key that can be inserted into the lock Figure 1.2. Although straightforward, they are hounded by significant flaws such as ease of replication, difficult tracking of utilization, and security compromise when a key is misplaced.

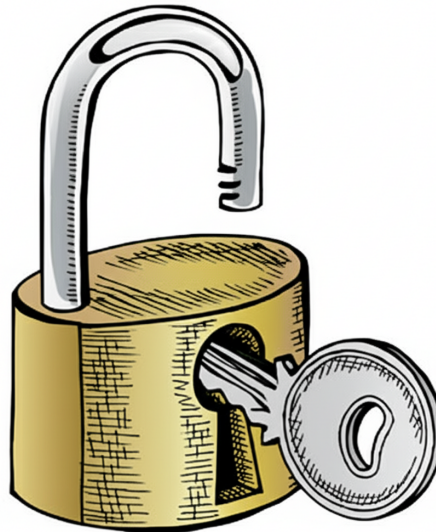


Figure 1.2: Mecanic Key

- **Magnetic Stripe Cards:** These cards were appearing in the middle of the 20th century with a magnetic stripe holding identification data. The card is swiped by a reader to unlock a door Figure 1.3. They were a step forward qualitatively in terms of ease of management but could be damaged and erased.

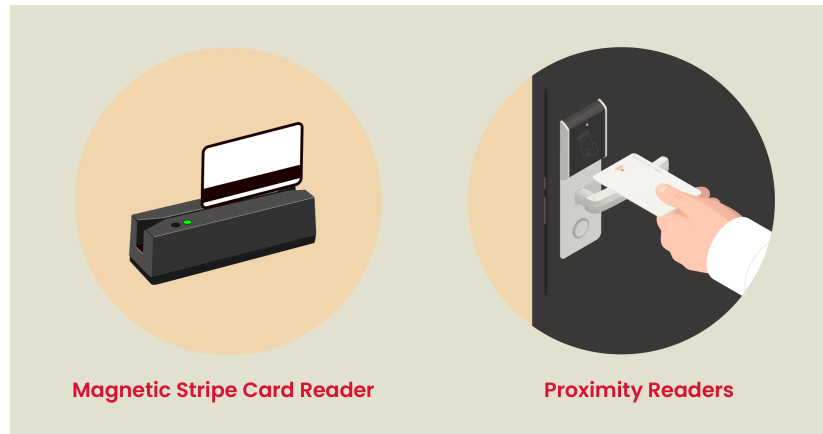


Figure 1.3: Magnetic Card

- **Smart Cards & NFC/RFID:** Around the end of the 20th century and beginning of the third millennium, Smart Cards began to be available in the marketplace with an electronic chip, subsequently followed by Near Field Communication (NFC) and Radio-Frequency Identification (RFID) technologies Figure 1.4. These technologies offer higher security, faster processing, and increased data storage capacity and do not require direct contact with the reader.



Figure 1.4: Smart Cards

- **Biometric Systems:** Are a qualitative leap in security because they rely on personal biological characteristics of an individual (fingerprints, iris scans, facial recognition, voice prints) Figure 1.5. Biometric systems reduce greatly the risk of impersonation and provide a high level of accuracy.
- **Network & Cloud-Based Access Control:** Over time, access control systems have evolved to become network-enabled (IP-Based), which allows for centralized control, remote monitoring, and integration with other security systems Figure 1.6. Cloud-Based ACS solutions are also there with more flexibility, lower maintenance costs, and accessibility from anywhere using the internet.

1.3 General Purposes of Access Control Systems

Access control systems play a significant role in the majority of environments for the achievement of strategic and continuous goals:

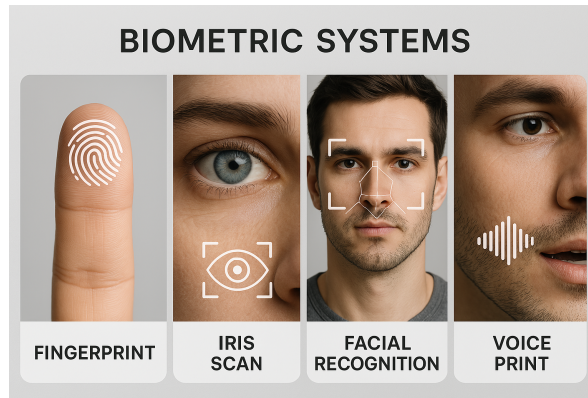


Figure 1.5: Biometric System

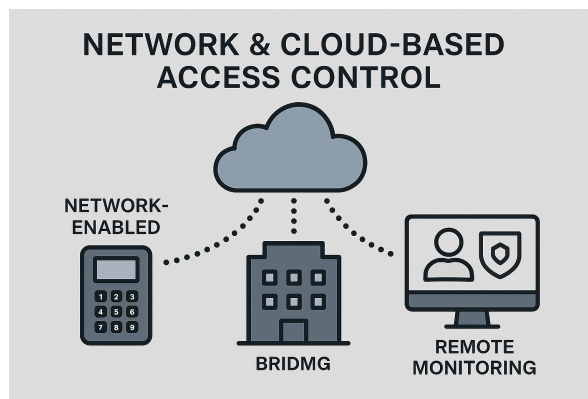


Figure 1.6: Cloud Access

1.3.1 Security & Defense

Access control systems play a pivotal role in strengthening the overall security posture of an organization or facility [4]. They serve not only to manage entry but also to enforce protective boundaries that shield people, assets, and information from internal and external threats.

- **Asset Protection:** Preventing unwanted access to physical assets (e.g., equipment, inventory) and data (confidential information).
- **Personnel Safety:** Stopping only approved individuals from entering certain areas, reducing security risk and safety occurrences.
- **Reduction of Crime:** Reducing opportunities for theft, vandalism, and sabotage.

1.3.2 Organization & Productivity

Beyond its security function, an access control system significantly contributes to the operational efficiency of an organization [5]. By automating and streamlining access processes, it enhances workflow, reduces administrative burden, and minimizes the risk of mismanagement in large and complex environments.

- **Improved Workflow:** Simplifying entry and exit mobility in large firms, reducing jams and confusion.

- **Centralized Control:** Allowing permissions to access for a large number of people and locations from a central point.
- **Reduced Human Error:** Automating the process of granting and denying access into one, reducing reliance on human intervention.

1.3.3 Auditing & Accountability

Access control systems not only regulate entry but also provide crucial support for auditing and traceability within organizations. By systematically recording access events, they enable administrators to reconstruct incidents, ensure policy compliance, and maintain organizational transparency.

- **Event Log:** Maintaining accurate and detailed records of every entry attempt (successful or failed), in terms of time, date, and identity of individual.
- **Investigations:** Enabling security investigations by the capacity to display who entered when and where, aiding in identifying responsibility.
- **Regulatory Compliance:** Helping businesses meet regulatory requirements and industry standards calling for accurate access logs.

1.3.4 Integration & Scalability

Modern access control systems are designed to operate not as isolated tools but as part of a broader ecosystem of security and management technologies. Their ability to integrate seamlessly with other systems and adapt to organizational growth ensures long-term usability and efficiency.

- **Integration with Other Systems:** The capacity to connect with other security systems such as Closed-Circuit Television (CCTV), fire alarm systems, and Building Management Systems (BMS) in order to offer a comprehensive and interactive security setting.
- **Ease of Expansion:** The ability to readily add new access points and users as the company grows.

Briefly, access control systems have become part of the modern security infrastructure, providing a vital layer of defense and helping organizations achieve higher levels of efficiency and accountability.

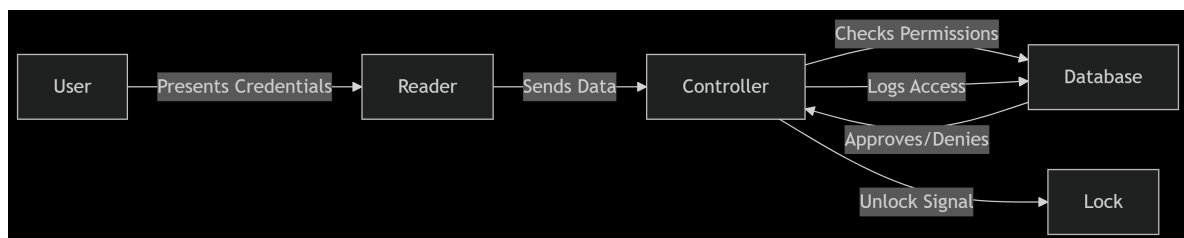


Figure 1.7: Components access control

1.4 The Importance of Access Management in Sensitive Environments (Laboratories as a Model)

Access management systems gain paramount importance in laboratories due to their sensitive nature, which demands high levels of security and control. This distinction stems from several fundamental aspects like show in the figure:



Figure 1.8: Risks Laborator

1.4.1 Protecting Valuable Resources and Assets

Laboratories serve as repositories for expensive scientific equipment (e.g., mass spectrometers, electron microscopes, chromatography systems), rare and hazardous chemical and biological materials, and invaluable research samples. Any unauthorized entry can lead to:

- **Theft or Damage:** The loss of equipment or destruction of samples can disrupt research for months or years, incurring significant financial losses. Access control systems, particularly those relying on **biometric verification** (e.g., fingerprint scanning), significantly reduce the risk of unauthorized entry compared to traditional methods vulnerable to lost keys or stolen cards.
- **Contamination or Misuse:** In chemical or biological laboratories, unauthorized access can lead to the contamination of experiments or the misuse of hazardous materials, potentially jeopardizing research results or causing accidents. For instance, a contaminant X introduced into a sterile environment could invalidate an entire batch of cell cultures, leading to a delay in research progress ΔT .

1.4.2 Ensuring Occupational Safety

Safety is a top priority in laboratories, especially those handling infectious biological agents, radioactive materials, or highly toxic chemicals. Access management systems ensure:

- **Restricting Access to Qualified Personnel Only:** The system can prevent individuals who have not received the necessary training to handle specific hazards, or who are not wearing appropriate **Personal Protective Equipment (PPE)**, from entering. This reduces incidents of exposure to hazardous materials or incorrect equipment operation.

- **Emergency Management:** In the event of an incident (e.g., a chemical spill or fire), the system can help identify the last individuals present inside the laboratory, facilitating evacuation and rescue operations and reducing risks to emergency responders. Knowing the precise location of personnel P_L at time t can significantly improve emergency response efficiency.

1.4.3 Protecting Intellectual Property and Data Confidentiality

Laboratories are vital environments for generating new knowledge and innovation. Ongoing research and preliminary results represent sensitive intellectual property that must be protected:

- **Preventing Information Leakage:** An access management system can restrict unauthorized individuals from viewing research manuscripts, experimental results, or confidential data stored within the laboratory. The integrity of research data is directly proportional to the effectiveness of access control.
- **Regulatory Compliance:** In certain industries (e.g., pharmaceuticals or defense), stringent levels of access control are required to comply with regulatory standards and laws related to data protection and intellectual property. Compliance with regulations like **Good Laboratory Practice (GLP)** or **Good Manufacturing Practice (GMP)** often mandates auditable access logs.

1.4.4 Effective Organization and Event Tracking

Modern access management systems allow for precise and comprehensive recording of all activities:

- **Entry and Exit Logs:** The system provides a detailed chronological record of who entered the laboratory and when, and who exited and when. This data is essential for **auditing**, assigning responsibility in case of incidents or breaches, and analyzing usage patterns to improve laboratory efficiency.
- **Dynamic Permissions Management:** Administrators can easily grant or revoke access privileges for each individual or group, specify certain entry hours, or restrict access to specific areas within the laboratory. This allows for flexible and adaptive control that can be adjusted to changing research needs. The permission set P_S for a user U can be dynamically updated based on their role R and current project needs N_P : $P_S(U) = g(R, N_P)$.

1.4.5 Challenges and Unique Requirements for Laboratories

While laboratories share the need for security with many other environments, there are specific requirements that distinguish them:

- **Cleanliness and Sterilization Requirements:** In biological or pharmaceutical research laboratories, some areas may require **Cleanrooms** that necessitate controlled entry to prevent contamination. Access management systems must integrate with sterilization protocols. The particle count N_P in a cleanroom must remain below a specified threshold, which is directly impacted by uncontrolled access.
- **Environmental Condition Monitoring:** Some laboratories require continuous monitoring of temperature (T), humidity (H), or air pressure (P_{air}). While access systems do not directly control these factors, they can integrate with monitoring systems to alert administrators in case of anomalies that might affect samples or equipment. For example, if $T > T_{\text{max}}$ or $H < H_{\text{min}}$, an alert is triggered.

- **Access Flexibility vs. Security:** Systems must balance providing flexible access for researchers and staff who need to work at irregular hours with maintaining the highest levels of security to prevent unauthorized entry. This requires a robust permissions management system that can be controlled remotely.

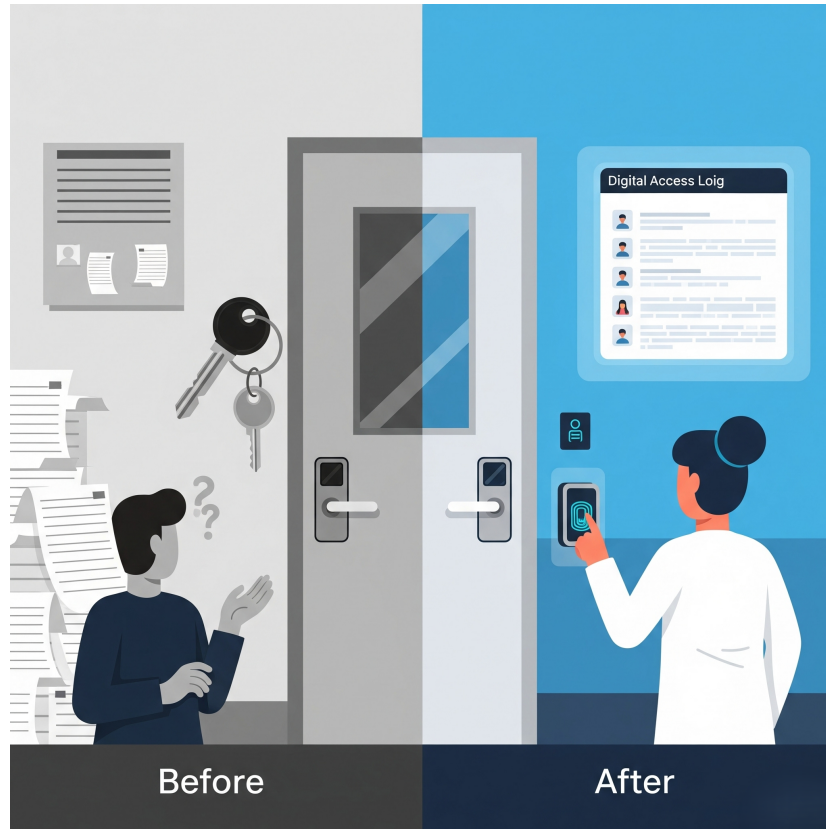


Figure 1.9: Befor/After access control

1.5 Modern Technologies in Smart Access Management Systems

This section introduces the key technologies that form the foundation of intelligent access management systems, providing a general overview without delving into specific implementation details.

1.5.1 The Concept of a "Smart System"

In the context of access management, a system is deemed "smart" when it exhibits capabilities beyond simple static authorization [6]. These capabilities include:

- **Adaptability:** The system's ability to adjust its behavior and rules based on changing environmental conditions, user roles, or security policies. This might involve dynamic permission adjustments or real-time threat assessment.
- **Automation:** The automatic execution of tasks, such as granting or revoking access, generating reports, or triggering alerts, without direct human intervention. This enhances efficiency and reduces human error.

- **Internet Connectivity:** The capacity to connect to the internet, enabling remote management, data synchronization, and integration with other networked services. This facilitates centralized control and distributed access points.
- **Data-Driven Decision Making:** The utilization of collected data (e.g., entry logs, sensor readings, anomaly detection) to inform and optimize access decisions, identify security vulnerabilities, or predict potential risks. This can be expressed as a function $D_{decision} = f(Data_{input})$, where f represents an analytical algorithm.

1.5.2 The Role of Central Web Servers

Central web servers form the backbone of a smart access management system, providing a robust and scalable infrastructure for system operation [7]. Their contributions include:

- **User Data Storage:** Securely storing and managing user profiles, credentials, access privileges, and biometric templates. This centralized repository ensures data consistency and integrity across all access points.
- **Event Logging:** Recording all access attempts, successful entries, denied requests, and system alerts in a comprehensive audit trail. This log is crucial for security analysis, compliance, and forensic investigations. Each event E_i can be timestamped and attributed to a specific user and access point: $E_i = (User_{ID}, AccessPoint_{ID}, Status, Timestamp)$.
- **Centralized Privilege Control:** Enabling administrators to define, modify, and revoke access permissions from a single, centralized interface. This ensures consistent policy enforcement and simplifies management across multiple locations or departments. The authorization matrix M_{Auth} can be managed and updated centrally, where $M_{Auth}(u, r)$ indicates if user u has access to resource r .

1.5.3 Web Applications

Web applications have become a prevalent choice for managing smart access systems due to their inherent advantages [8]:

- **Ubiquitous Accessibility:** They can be accessed from any device with an internet connection and a web browser, eliminating the need for specialized client software installations. This provides unparalleled flexibility for administrators.
- **Graphical User Interface (GUI):** Offering intuitive and user-friendly graphical interfaces that simplify complex management tasks, making the system accessible to a wider range of users without extensive technical training.
- **Ease of Updates and Maintenance:** Updates and new features can be deployed centrally on the server, immediately becoming available to all users without requiring individual client-side installations. This streamlines maintenance and ensures all users are on the latest version.

1.5.4 Internet of Things (IoT) in Access Management

Internet of Things (IoT) devices bridge the gap between the physical environment and the digital access management system. Microcontrollers like the **ESP32** are exemplary in this role due to their integrated Wi-Fi and Bluetooth capabilities [7]. Their contributions include:

- **Sensor Reading:** Collecting real-time data from various sensors (e.g., door status, motion detection, environmental parameters) to provide contextual information for access decisions and security monitoring.
- **Lock Control:** Directly interfacing with electronic locks and other physical access mechanisms to grant or deny entry based on authorization signals received from the central server.
- **Network Communication:** Facilitating secure communication between physical access points and the central web server, transmitting authentication requests, event logs, and receiving commands. This communication often occurs over secure protocols like HTTPS or MQTT. The data flow can be represented as

$$Data_{IoT} \xrightarrow{\text{Network}} Server \xrightarrow{\text{Command}} Actuator$$

1.5.5 Biometric Authentication Technologies

Biometric authentication offers a highly secure and convenient method for identity verification, leveraging unique physiological or behavioral characteristics. **Fingerprint recognition** is a prominent example:

- **Security:** Fingerprints are unique to each individual, making them difficult to forge or replicate Figure 1.10. This provides a higher level of assurance compared to traditional methods.
- **Convenience:** Users do not need to carry physical keys or cards, reducing the risk of loss or theft. The authentication process is typically quick and seamless.
- **Comparison to Traditional Methods:**
 - **Keys:** Prone to loss, theft, and unauthorized duplication. No audit trail.
 - **Access Cards:** Can be lost, stolen, or shared. May require physical contact or proximity. Offers an audit trail but less secure than biometrics without additional factors.

Biometric systems offer a significant enhancement in both security and user experience, often providing an immutable link between the user and their access rights.

1.5.6 Additional Verification Methods

While biometrics offer strong primary authentication, incorporating additional verification methods enhances security and provides fallback options:

- **Keypad (PIN Code):** A keypad serves as an additional layer of security, requiring users to enter a Personal Identification Number (PIN) in conjunction with a biometric scan (multi-factor authentication). It can also function as a standalone alternative in scenarios where biometric authentication is temporarily unavailable or undesirable. The authentication process can be defined as $Auth = Biometric \wedge PIN$, requiring both factors to be true for access.

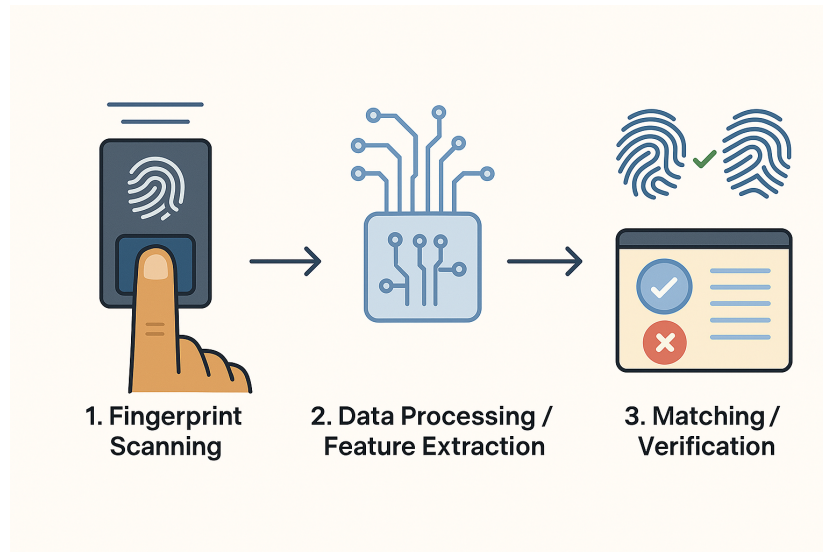


Figure 1.10: Biometric Process

1.6 Conclusion

In this first chapter, we have broadly reviewed the significance of Access Management Systems (AMS) and specifically highlighted their vital role in safeguarding and securing sensitive environments, particularly laboratories. It has become evident that laboratories are not merely places for conducting experiments; they are centers for safety, security, and the protection of intellectual property, demanding advanced solutions that transcend traditional control methods. We also shed light on the transition towards smart systems, empowered by technologies such as the Internet of Things (IoT), centralized servers, and biometric verification methods, which promise to deliver unprecedented levels of efficiency, accuracy, and security. Despite the clear technological advancements and the emphasis on the necessity of implementing smart Access Management Systems, the practical application of these solutions in real-world environments, especially within the context of our local laboratories, still faces specific challenges. These challenges are not limited solely to the technical aspect concerning the integration of various components, such as ESP32 with a Flask server and fingerprint recognition, but extend to encompass aspects of operational efficiency, ease of remote management, and the costs associated with practical implementation. Hence, the question arises regarding the effectiveness of currently available solutions in meeting the specific requirements of modern laboratories. Furthermore, it prompts us to consider how a smart system can be designed to combine the highest degrees of security and flexibility, while maintaining ease of use and management. This directly leads us to the second chapter, where we will thoroughly articulate the problem statement that this research project seeks to address and identify the gaps we aim to bridge through the proposed solution.

Chapter 2

Project Motivation and Problem Statement

2.1 Introduction

Building on the theoretical foundations and classifications of access control systems discussed in the previous chapter, it becomes increasingly clear, particularly in the context of technological advancements and growing security demands in educational environments, that the practical implementation of intelligent access control is both timely and necessary. This chapter presents the motivations that underpin the development of a smart access management system tailored to the specific operational context of the Faculty of Science and Technology. The faculty serves as a compelling case study due to its complexity as a higher education and research institution, with diverse infrastructures and access requirements. It encompasses four lecture halls with a combined capacity of 800 seats, 16 teaching rooms of varying sizes, and a network of pedagogical laboratories accommodating up to 570 students simultaneously. In addition, the faculty includes specialized research spaces such as an innovation lab for 15 researchers, two scientific labs each accommodating 70 researchers, and a 75-seat hall dedicated to academic defenses and presentations.

This broad array of spaces and uses creates a multifaceted, layered security challenge. The diversity of users, from large, fluctuating student populations and mobile faculty researchers to administrative personnel and external guests, requires tailored access strategies. At the same time, the range in facility sensitivity levels further complicates security needs: while classrooms require standard protection, pedagogical labs house specialized equipment, research labs contain advanced and sensitive materials, and server rooms support critical network infrastructure. Managing the flow of more than 1,500 individuals daily across a distributed campus places significant strain on existing access systems. Current conventional methods fail to enable dynamic access control, efficient crowd management during peak hours, and accurate tracking of personnel and equipment usage. These operational challenges highlight the need for a robust, adaptive, and scalable access control solution that is aligned with the structural diversity and functional complexity of the faculty.



Figure 2.1: Faculty of Science and Technology

2.2 Current Situation Analysis in the College of Science and Technology, Challenges and Costs

The College of Science and Technology continues to rely on a traditional system due to the absence of a sophisticated and smart access control system. The process is largely dependent on human personnel for managing entry and exit operations to various educational and research facilities. Although this method offers a basic level of general security, it presents numerous challenges related to economic cost, operational efficiency, and resource management.

2.2.1 Human Resource Allocation for Access Control and Security

An analysis of the human resources involved in access control and security reveals a complex and structured organization comprising both administrative and technical personnel. In total, fifteen staff members are assigned to various functions ranging from general administration to highly specialized engineering roles. At the upper management level, a general engineer oversees the general supervision of the limited technical infrastructure, while one laboratory engineer coordinates access to critical laboratory environments. Supporting them are four specialized engineers and one staff member focused specifically on laboratory administration, reflecting the institution's strong commitment to safeguarding sensitive research areas and high-value equipment.

At the operational level, the structure includes four university laboratory technicians responsible for routine maintenance and system monitoring, along with three senior laboratory technicians who provide advanced technical assistance. In addition, the general affairs department contributes two personnel, one senior technician and one technician, tasked with the daily management of access control operations. This layered distribution of responsibilities ensures a balanced approach to both strategic oversight and hands-on implementation within the access control system.

2.2.2 Financial Analysis of Current Costs

The financial burden of this human-based access control system is significant and calls for a strategic reevaluation. According to the Algerian public sector salary scale, monthly costs amount to approxi-

mately 5.5 million centimes for the state engineers and 3.5 million centimes for the technicians involved in security and access control operations.

Position	Number	Monthly Salary (DZD)	Monthly Cost (DZD)	Annual Cost (DZD)
State Engineer in General Affairs	1	55,000	55,000	660,000
Engineer for University Laboratories	1	55,000	55,000	660,000
State Engineer in University Laboratories	4	55,000	220,000	2,640,000
University Laboratory Technician	4	35,000	140,000	1,680,000
Senior Technician in University Laboratories	3	35,000	105,000	1,260,000
Senior Technician in General Affairs	1	35,000	35,000	420,000
Technician in General Affairs	1	35,000	35,000	420,000
Total	15	—	645,000	7,740,000

Table 2.1: Monthly and Annual Costs of Access Control Staff (in Dinar)

Current Situation Analysis in the College of Science and Technology: Challenges and Costs Annual Financial Burden These amounts demonstrate the following shocking reality: the college is spending, every year, a sum nearly equal to **774 million Algerian centimes** (or **7.74 million Algerian dinars**) in simple wages regarding human resources allocated for security and access control duties. This enormous sum constitutes a genuine burden on the college's financial resources, particularly given that most of these duties can be more effectively and cheaply achieved in the long run.

FST Ghardaïa Structure

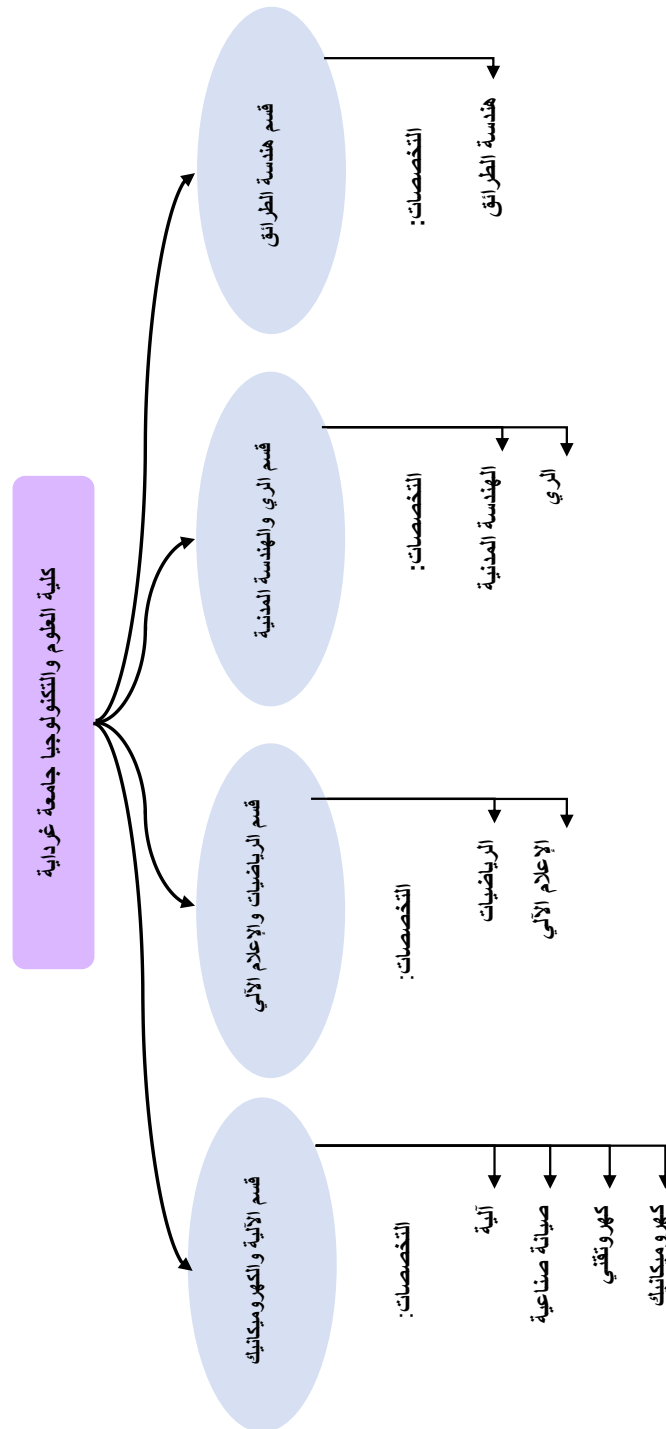


Figure 2.2: Organizational Chart of the Faculty of Science and Technology

2.2.3 Administrative and Operational Challenges

The current access management approach within the Faculty of Science and Technology is heavily reliant on human intervention, which introduces a range of administrative inefficiencies. The coordination of fifteen staff members across multiple facilities and rotating shifts presents a persistent challenge, often leading to miscommunication, inconsistent coverage, and operational bottlenecks. In addition, the traditional system lacks a centralized infrastructure to monitor entry and exit activity, making it difficult for administrators to base decisions on reliable data. The process is reactive rather than preventive, with issues addressed only after they arise. Manual access control also means that the institution has little visibility over who is entering its facilities, when they are doing so, or for what purpose, which compromises both security and resource management. The existing model, based on guards and manual keys, is no longer suitable for a technologically advanced academic institution, especially one that requires high levels of accountability, traceability, and operational responsiveness.

One of the most visible consequences of this outdated system is the under-use or mismanagement of laboratory equipment. Without a centralized and intelligent access tracking system, equipment availability often becomes unclear, leading to cases where valuable resources are idle, misused, or damaged due to neglect. A major contributing factor is the lack of updated, transparent information regarding what equipment is available and where, resulting in many users remaining unaware of accessible resources. Moreover, in the absence of logging mechanisms, it becomes nearly impossible to assign responsibility in the event of misuse or loss. This has fostered a culture of negligence, where accountability is diminished and maintenance is often deferred. Financially, the institution continues to invest in personnel without proportional returns in security or administrative efficiency. In addition, students and faculty report a general sense of insecurity due to the lack of controlled access and audit trails, discouraging some users from using facilities altogether for fear of being blamed for incidents they did not cause. Collectively, these issues underscore the urgent need for an intelligent access system capable of improving oversight, ensuring accountability, and optimizing the use of human and material resources.

2.3 Problem Statement

The Faculty of Science and Technology faces serious challenges in managing physical access to its buildings, laboratories, and administrative offices. The current infrastructure relies heavily on traditional methods that are increasingly inadequate for a modern academic institution that accommodates hundreds of students, staff, and researchers per day. At the core of the issue lies the need to design a comprehensive smart access control system that integrates multiple critical requirements, security, flexibility, automation, and administrative simplicity, without compromising operational efficiency. Security remains the highest priority due to the presence of sensitive research instruments, valuable equipment, confidential academic records, and intellectual property, all of which are vulnerable under the existing access system. In addition, human-dependent procedures cause delays and inconsistencies, especially during peak hours, while also increasing the risk of operational failures when key personnel are unavailable.

Beyond the security implications, the current system also imposes a significant financial burden through ongoing personnel costs and the maintenance of outdated infrastructure. This diverts funding away from core educational and research missions. In addition, manual entry logs do not deliver the accuracy and detail needed for security audits, emergency preparedness, or space usage analysis. This lack of reliable tracking impairs decision-making and investigative processes. The problem is

further compounded by the dynamic nature of academic environments, where student enrollments, staff assignments, and research collaborations frequently change. Consequently, the system must support scalable and flexible user management, enabling administrators to easily grant, update, or revoke access rights while preserving a detailed record of all actions. These combined challenges highlight the urgent need for an intelligent, centralized, and adaptive access control solution.

2.3.1 Reasons for Selecting the Solution

The current access control system in the Faculty of Science and Technology has a number of operational and cost problems necessitating immediate modernization. A critical study of the current system reveals systemic inefficiencies that impact security effectiveness as well as operation costs.

Human Resource Allocation and Cost Implications

The personnel now include a significant proportion of security guards whose principal responsibility rests with monitoring entrance operations at various entrance points. These types of staff costs are a significant part of operating expenditure, not only including base salaries but also corresponding benefits, training fees, overtime rates, and replacement fees in case of absence. The financial implication does not end with the direct payment to reach supervision overhead, scheduling coordination, and performance management requirements. This staff-intensive model generates repeat cost obligations that increase annually with salary hikes and benefit cost hikes, producing an unsustainable strategy for long-term budgeting. Moreover, the human-dependent system provides operational vulnerabilities in times of staff shortages, sick leave, or turnover situations. The building often has security gaps when personnel are not present, requiring temporary closure of openings or penalizing security procedures. Recruitment and training of alternate security staff take longer and manpower, bringing additional cost issues.

Equipment Management and Asset Protection

The current infrastructure is beset by significant equipment loss, damage, and misuse issues. Traditional key-based access control mechanisms result in repeated duplication of keys, lost keys that result in lock replacements, and invisibility of key issuance. All these problems do not only pose security threats but also generate repeated replacement costs and administrative overheads. Physical access badges and cards have high unauthorized copying rates, damage rates, and loss rates. Replacing them involves administrative time, material, and temporary security compromises while new credentials are being created. Furthermore, the inability to monitor in real time implies stolen or lost access credentials may stay active for extended periods of time, hence still remaining a security threat.

Administrative Efficiency and Control Limitations

Individual administrative action under the current system is insufficient to guarantee unified and efficient access control across the heterogeneously different facility environment. Issuance, modification, and revocation of access privileges through manual methods are given delays, increase the likelihood of errors, and complicate the maintenance of contemporary records of prevailing levels of authority. The management overhead of coordinating access permissions across departments, research groups, and user categories consumes significant staff time and creates operational bottlenecks. The lack of centralized management tools means that multiple administrators must coordinate changing access, introducing complexity and delay to make routine adjustments. The need for a secure, central system in real-time has become critical since the operations of the faculty are becoming increasingly complex and security-related. The current distributed approach to access control makes it difficult to maintain

security policies consistent, monitor access patterns, or respond to security violations promptly. Real-time monitoring capabilities are required to discover unauthorized access attempts, identify unusual access patterns, and provide timely warning in the event of security breach. The absence of real-time feedback and monitoring in the current system leaves the faculty open to unnecessary security breaches that could be prevented or minimized with proper technological infrastructure. Educational facilities today require full electronic records of access activity to facilitate security auditing, compliance reporting, and operations analysis. Electronic privilege delegation and automated entry logging are the foundations for sophisticated security analytics that allow administrators to spot potential security risks, optimize facility utilization, and demonstrate compliance with institutional security procedures. The shift to electronic access management also supports integration with other institutional systems, such as student information systems, human resources databases, and facility management systems. The ability to integrate creates the potential for higher operational efficiency and higher security through coordinated data sharing and automated policy enforcement.

2.4 Orientation Toward the Proposed Solution

To the needs and challenges that have been identified, we propose the design and implementation of a complete smart access control system that exploits advanced security technologies and centralized management functions. This is a move away from traditional, human-centric access control modes to an automated, technology-centric system that is able to cure the current weaknesses of the faculty with the provision for expansion with future development. Technology Integration and Multi-Modal Authentication The system integrates multiple authentication models for strong security with the flexibility to support different user preferences and accessibility needs. PIN code is a convenient and easy access mechanism for frequent entries, whereas biometric fingerprint recognition is more secure for areas needing a higher level of protection. The system design supports additional authentication factors like proximity cards, mobile integration, and face recognition capabilities for flexible deployment according to particular security requirements for individual facility areas. The multi-modal component enables the system to accommodate users with varying levels of comfort in using technology without any compromise on security levels. All authentication information is secured by advanced encryption standards during data transmission and storage, safeguarding biometric and personal information from potential cyber attacks.

2.4.1 Centralized Management and Real-Time Operations

Centralized architecture provides the administrators with end-to-end control of access permissions, monitoring capabilities, and system configuration through an intuitive web-based management console. Real-time processing ensures immediate authentication responses to prevent latency during high usage periods while providing instant alerting on unauthorized access attempts or system issues. The database maintains very detailed records of each access event, from successful access to failed login and sys admin updates to user privileges. Such comprehensive logging capability enables comprehensive security audits, helps identify patterns that may be indicative of security threats, and provides the data necessary for maximizing facility utilization based on actual usage patterns.

2.4.2 Automated Monitoring and Intelligent Analytics

Advanced monitoring capabilities continuously analyze patterns of access in an effort to detect abnormal behavior that could indicate security or operational issues. Activity such as attempts at access during non-work hours, repeated rapid attempts at access, or access patterns that are outside normal

patterns of expected user activity are detectable using machine learning algorithms. The system offers auto-administrative review reports, which pinpoint the most important security metrics, system performance indicators, and operational improvement suggestions. Integration with the existing institutional communication infrastructure provides for notification of security incidents to the concerned personnel in real-time, enabling quick reaction to potential threats.

2.4.3 Scalability and Future-Proofing

The solution design envisioned offers transparent scalability to accommodate growth in facilities, user base, or increased security requirements. Modular design allows for the incorporation of new authentication mechanisms, support for integration, or functional additions without requiring complete system replacement. Cloud-based components provide space for remote system management, off-site backup, and interaction with other institutional systems. The approach reduces local infrastructure requirements without sacrificing system reliability and data protection by expert cloud service providers.

2.4.4 Implementation Strategy and Change Management

The deployment model is based on phased release in order to minimize operational disruption and allow system optimization based on real-world usage trends. Phased deployment begins with lower-priority access points, followed by staff and user exposure to the new system prior to deploying within high-security areas. Comprehensive training of administrators and end-users promotes easy uptake and maximizes the system's effectiveness. System maintenance and technical support mechanisms guarantee long-term reliability and future scope for improvement through user feedback and evolving security requirements. This proposed intelligent access control system is an end-to-end solution that addresses the immediate needs of the faculty and is the foundation for future security and operations improvement. The combination of state-of-the-art technology, centralized administration, and adaptable architecture ensures that the investment will pay dividends as the institution's requirements evolve over the years .

2.5 Conclusion

This chapter outlined the foundational motivations for developing an intelligent access control system within the Faculty of Science and Technology. Through an analysis of human resources, financial constraints, and organizational challenges, the current limitations of existing access practices were clearly identified. A structured problem statement was formulated, highlighting the need for a secure, scalable, and manageable solution. Furthermore, the orientation toward a proposed system was established, setting the stage for the technical development presented in the following chapters.

Chapter 3

Hardware Design for Secure Access Control

3.1 Introduction

The effectiveness of any access control system is fundamentally dependent on the robustness of its hardware design. In the proposed system, hardware is not merely a supportive layer, but a central element that enables secure, real-time decision making at the physical access point. It must reliably handle tasks such as identity acquisition, local data processing, network communication, and actuation of access mechanisms. To meet these requirements, the system integrates a carefully selected set of electronic components, with the ESP32 microcontroller at its core. Known for its high processing capability and built-in Wi-Fi support, the ESP32 serves as the central processing unit responsible for coordinating interactions between all subsystems.

Complementing the microcontroller are additional components that ensure the system's full functionality: a fingerprint sensor for biometric authentication, a 4x3 keypad for PIN-based access, a relay module to trigger door locking mechanisms, a buzzer to provide real-time audio feedback, and a stable power supply to guarantee uninterrupted performance. The overall hardware architecture is designed to be compact, energy efficient, and cost effective, without compromising on reliability or security. Each component was selected based on its functional contribution, ease of integration, and compatibility with embedded systems for secure access control. The following sections provide detailed explanations of each component's role, selection criteria, and integration into the complete hardware setup, demonstrating how the hardware layer supports the operating goals of the system.

3.2 System Components

The implementation of the proposed access control system required the integration of several electronic and electromechanical components, each chosen to fulfill a specific role in ensuring secure authentication, user interaction, and control of the access mechanism. At the heart of the system lies the ESP32 microcontroller, which handles data processing and communication tasks. A fingerprint sensor provides biometric authentication, while a 4x3 matrix keypad serves as an alternative or complementary method for PIN-based user verification. Access control is physically managed through a relay module that activates or deactivates the door locking mechanism based on authentication outcomes. To improve the user experience, a buzzer provides audible feedback indicating successful operations or errors. The power to the system is supplied by a regulated 5V source to maintain stability and relia-

bility across all components. The integration is supported by connecting wires and auxiliary electronic elements, which ensure proper communication and functionality between the various modules.

3.2.1 ESP32 Development Board

The ESP32 development board is a powerful and cost-effective microcontroller platform based on a dual core system-on-chip with built-in Wi-Fi and Bluetooth, making it highly suitable for Internet of Things (IoT) applications. Its low power consumption, excellent wireless capabilities, and extensive input/output (I/O) support enable seamless integration with a wide range of sensors and actuators. In this project, the ESP32 serves as the central processing unit and communication hub, responsible for collecting sensor data, managing access logic, triggering output devices, and maintaining Wi-Fi connectivity for real-time monitoring. The board supports popular development frameworks such as the Arduino IDE and ESP-IDF, allowing for flexible and efficient programming. One of its most critical features is its advanced interrupt management system, which enables real-time responsiveness to events like fingerprint scans or keypad inputs without continuous polling, optimizing system performance and reliability.

As illustrated in Figure 3.1, the compact layout and versatility of the ESP32 make it an ideal choice for embedded access control systems. Its rich set of GPIO pins, analog-to-digital converter (ADC) channels, and communication interfaces (SPI, I2C, UART) allow for reliable connections to peripherals such as biometric sensors, keypads, buzzers, and relays. The board's design supports energy-efficient operation, making it suitable for battery-powered deployments, and is backed by strong community support and extensive documentation. A detailed pinout diagram, shown in Figure 3.2, provides essential reference to establish accurate hardware connections, with color-coded indicators for functionalities such as PWM, touch sensors, and communication lines. These features collectively position the ESP32 as a robust and scalable solution for intelligent access control applications.

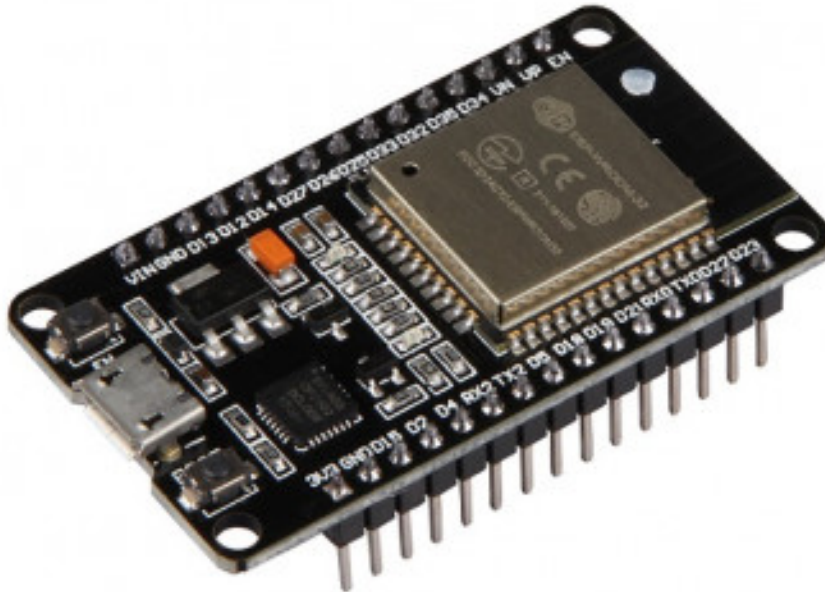


Figure 3.1: esp32 board

ESP32 WROOM 32E Pinout

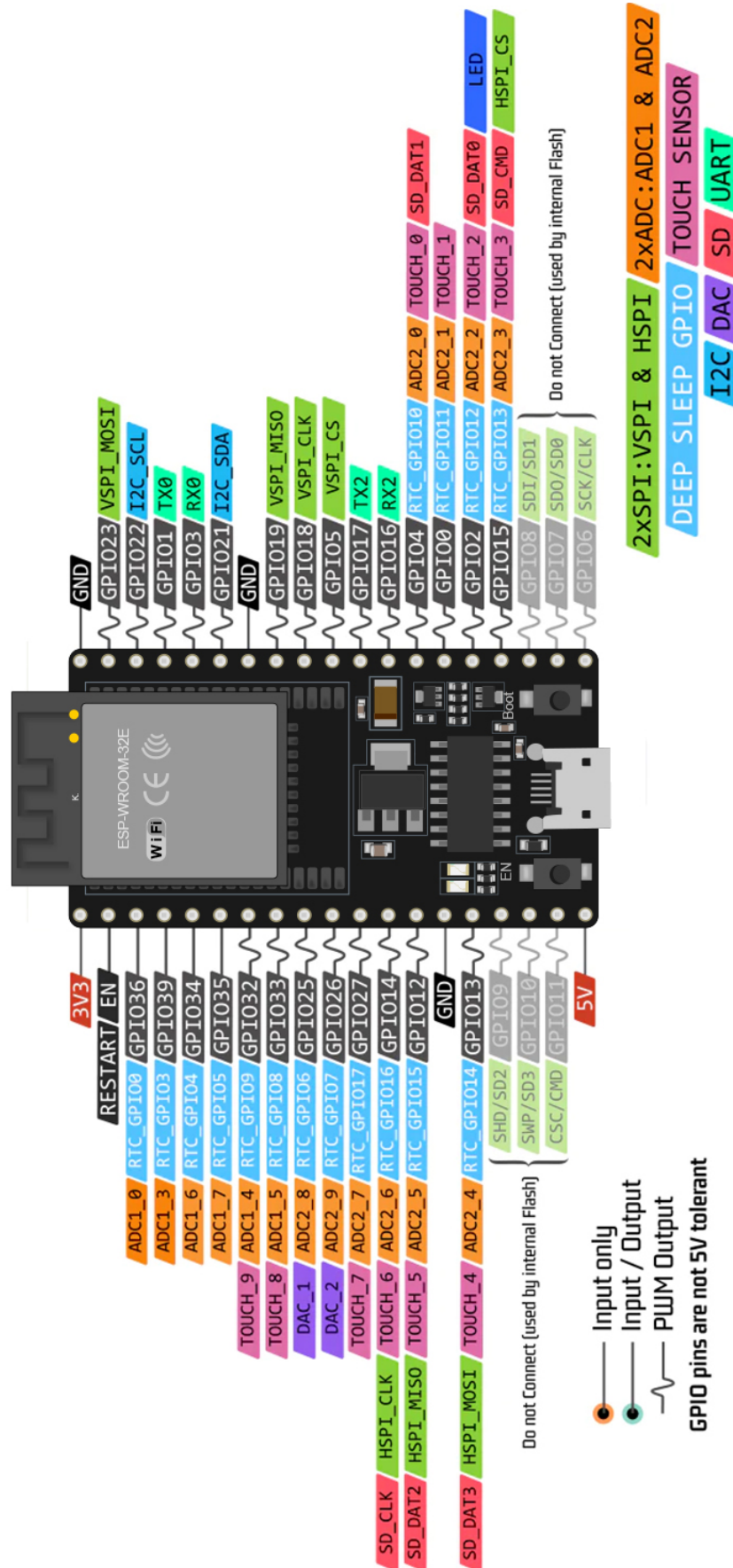


Figure 3.2: ESP32 WROOM 32E Pinout Diagram

3.2.2 Fingerprint Reader Module

A fingerprint reader module is a biometric device designed to capture, analyze, and store fingerprint patterns for the purpose of identification or authentication. Widely used in security systems, these modules offer an efficient and reliable method of verifying an individual's identity. Common modules such as the AS608 Figure 3.3. or R305 utilize optical sensors to capture high-resolution fingerprint images. Once a fingerprint is placed on the sensor surface, the module internally processes the image to extract unique features such as ridges, valleys, and points of interest. These features are then converted into a mathematical representation known as a template, which is stored in the module's memory and associated with a unique identification number (Template ID). During subsequent scans, the module compares the new fingerprint data with the stored templates through verification (one-to-one) or identification (one-to-many) processes [9].



Figure 3.3: AS608 Fingerprint Reader Module

The actual fingerprint image is not stored, ensuring a higher level of privacy and data security. Instead, the system refers to the corresponding ID to determine whether access should be granted. These modules are favored in embedded systems because of their built-in microcontroller for processing, ease of integration through UART communication Figure 3.4, compact size, and cost-effectiveness. They also offer sufficient internal storage to accommodate between 100 and 150 fingerprint templates, making them highly suitable for access control, time attendance, and personal authentication applications [10].

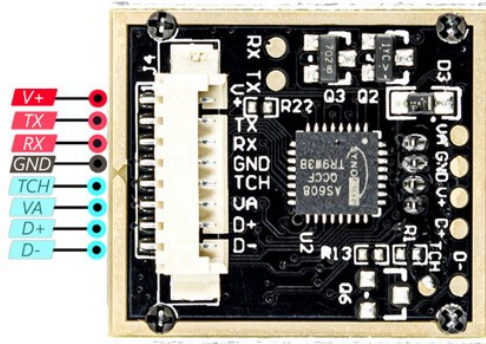


Figure 3.4: AS608 Fingerprint Module Pinout Diagram

Wiring the AS608 Fingerprint Module to the ESP32 Microcontroller

Establishing a reliable hardware connection between the AS608 fingerprint module and the ESP32 microcontroller is crucial to the functionality of biometric authentication systems. The AS608 module operates with a voltage requirement of 3.3V, which aligns with the logic level of ESP32, eliminating the need for additional voltage regulators or level shifters [11].

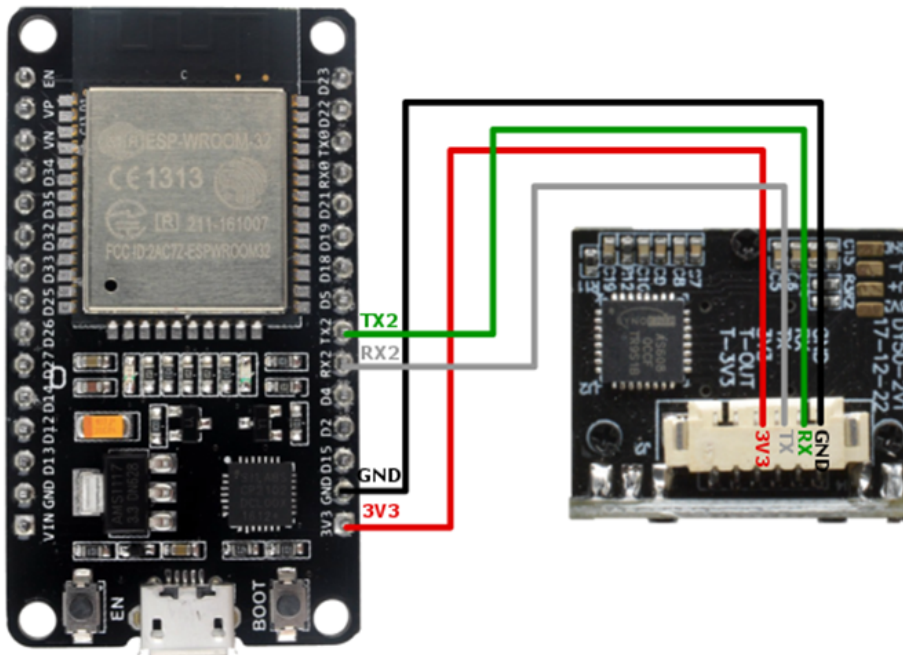


Figure 3.5: Wiring diagram of the AS608 fingerprint module connected to the ESP32

To power the module, its **VCC** pin is directly connected to the **3.3V** output pin of the ESP32, while the **GND** pin is linked to the ESP32's **GND** to provide a stable power supply and a common reference ground essential for consistent signal transmission. For data communication, the AS608 employs the **UART (Universal Asynchronous Receiver/Transmitter)** protocol. In this setup, the **TX** pin (responsible for transmitting data from the module) is connected to **GPIO16 (RX2)** of the ESP32, and the **RX** pin (used to receive data) is connected to **GPIO17 (TX2)** as shown in Figure 3.5. These GPIO pins correspond to the second hardware serial interface (**Serial2**), which is particularly useful when the primary serial port is occupied (for example, for USB debugging). This configuration allows full-duplex serial communication between the ESP32 and the AS608 module at a typical baud rate of **57600 bps**, although this can be configured in software. Proper UART wiring ensures that the ESP32 can issue commands for fingerprint registration, search, deletion, and comparison, while also receiving fingerprint templates and acknowledgment responses. The reliable setup of this serial link is essential for the security, performance, and responsiveness of the entire access control system, as summarized in Table 3.1.

AS608 Pin	ESP32 Pin
VCC	3.3V
GND	GND
TX	GPIO16 (RX2)
RX	GPIO17 (TX2)

Table 3.1: Pin connections between AS608 and ESP32

3.2.3 Understanding and Operation of a 3x4 Matrix Keypad

A 3x4 matrix keypad is a common and basic human-machine interface component in many embedded systems and electronic devices. It is especially crucial in systems where numeric data input is required, such as security systems, calculators, electronic locks, and devices that require menu input. The keypad is an array of twelve individual tactile push buttons shaped into a three-by-four matrix. Each button is located at the intersection of a specific row and column, producing a structured grid pattern [12]. This matrix configuration (Figure 3.6) is used to reduce the quantity of I/O pins needed from a microcontroller. Instead of using twelve separate pins, one for every button, the matrix configuration wonderfully reduces the number of I/O lines needed to seven: four for the columns and three for the rows. This significantly saves pin resources in microcontrollers and is ideal for projects with limited hardware resources. When a key is pressed, it links one row to one column. Scanning the rows and columns programmatically, the microcontroller can precisely observe which key was pressed. Rows are typically set up as output and columns as inputs (or vice versa), and software cycles through the rows and observes the input columns for state changes in signal. The keypad is usually made of durable plastic and utilizes membrane or mechanical switches to sense presses, providing responsive tactile feedback. Libraries and routines are readily available for popular development platforms such as Arduino, making integration straightforward for new developers and experts alike. The tiny size, efficient build, and ease of use make the 3x4 matrix keypad a go-to option for adding numeric or command input to numerous electronic devices.



Figure 3.6: 4x3Keypad Module

Internally, the keypad uses a network of conductive traces and momentary switches. These switches are normally open, which means that in their idle state, there is no electrical continuity between any row and column. When a user presses a button, the switch is mechanically closed at that intersection point, completing an electrical connection between the corresponding row and column lines. To detect this event, the microcontroller engages in a method known as keypad scanning. In this process, the row pins are set as digital output, and the column pins are configured as digital input (Figure 3.7), typically with internal or external pull-up resistors to ensure a default HIGH state. The scanning routine involves setting one row at a time to a LOW voltage while keeping the other rows HIGH and immediately reading the logic states of the column inputs. If a column line reads LOW during this cycle, it indicates that the button at the junction of the currently active row and that specific column is being pressed. For example, if the second row (row 2) is driven LOW and the microcontroller detects that the second column (column 2) has also gone LOW, it concludes that the button at the intersection of row 2 and column 2—typically representing the '5' key in standard layouts—has been actuated. The exact key is then identified using a predefined lookup table (keymap) that maps row-column pairs to characters or functions. This row-by-row scanning continues in a loop, allowing for real-time detection of any key press with minimal latency. Debouncing techniques, either in software or hardware, are generally applied to prevent false triggers due to mechanical vibrations when the button is pressed or released [13].

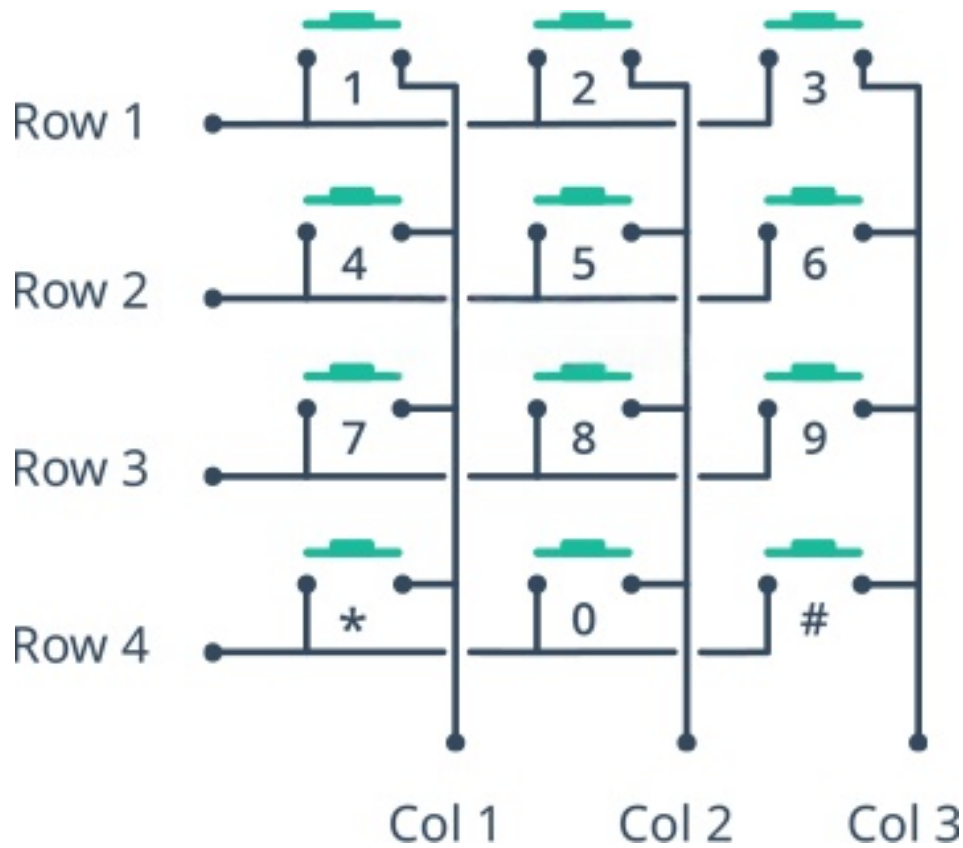


Figure 3.7: 4x3 Keypad Arrangement

This scanning mechanism makes the 3x4 matrix keypad both space-efficient and cost-effective, particularly in microcontroller-based designs where I/O availability is limited. Its simplicity, reliability, and low power requirements contribute to its popularity in a wide range of digital systems, including security systems, access control units, handheld devices, vending machines, and industrial control panels. In our access control system, which integrates fingerprint recognition and keypad input, the inclusion of the 3x4 matrix keypad serves a critical role in enhancing security, flexibility, and system reliability. While the fingerprint sensor provides biometric authentication based on unique physiological traits, the keypad offers an additional layer of verification through the input of personal identification numbers (PINs) or access codes. This dual-factor authentication approach strengthens the overall security framework by requiring both "something you are" (fingerprint) and "something you know" (PIN). Furthermore, the keypad allows for manual override or alternative access methods in cases where the fingerprint sensor does not recognize a user due to dirt, injury, or sensor malfunction. It also facilitates administrative tasks such as user enrollment, system configuration, and temporary access control without the need for a separate interface. From a design perspective, Figure 3.8, the compact matrix layout of the keypad is suitable for embedded systems with limited I/O resources, and its low power consumption complies with the energy-efficient requirements of our application. These advantages make the keypad a strategic and essential component of our system, contributing to both usability and operational robustness.



Figure 3.8: 4x3 Membrane Keypad Pinout

Wiring a 3x4 Matrix Keypad to an ESP32 Microcontroller

To establish effective communication between a 3x4 matrix keypad and an ESP32 microcontroller, a systematic wiring configuration is essential to correctly map the twelve keys of the keypad to the microcontroller's digital input/output (I/O) pins Figure 3.9 . The keypad itself is structured with four row lines and three column lines, making a total of seven signal lines that need to be interfaced with the ESP32. In this specific set-up, the row lines (typically labeled R1 to R4) are connected to GPIO pins 12, 14, 27, and 26 on the ESP32, respectively. Similarly, the column lines (C1 to C3) are connected to GPIO pins 25, 33, and 32 Table 3.2 . This pin mapping allows the microcontroller to scan the keypad by sequentially activating each row line and monitoring the column lines for any changes in voltage levels that would indicate a button press. Each button press creates a connection between a specific row and column line, which the ESP32 identifies by comparing the active row with the column that registers a LOW signal. The code snippet provided initializes a two-dimensional array, `keys[ROWS][COLS]`, representing the layout of characters on the keypad: from '1' to '9', with '*', '0' and '#' on the bottom row. This logical mapping is crucial for the ESP32 to interpret electrical signals as human-readable characters. By combining this wiring configuration with a keypad library and a

scanning routine, the ESP32 can detect and respond to user input accurately, allowing the keypad to function as a reliable interface for numeric entry, access control, or menu selection in embedded applications.

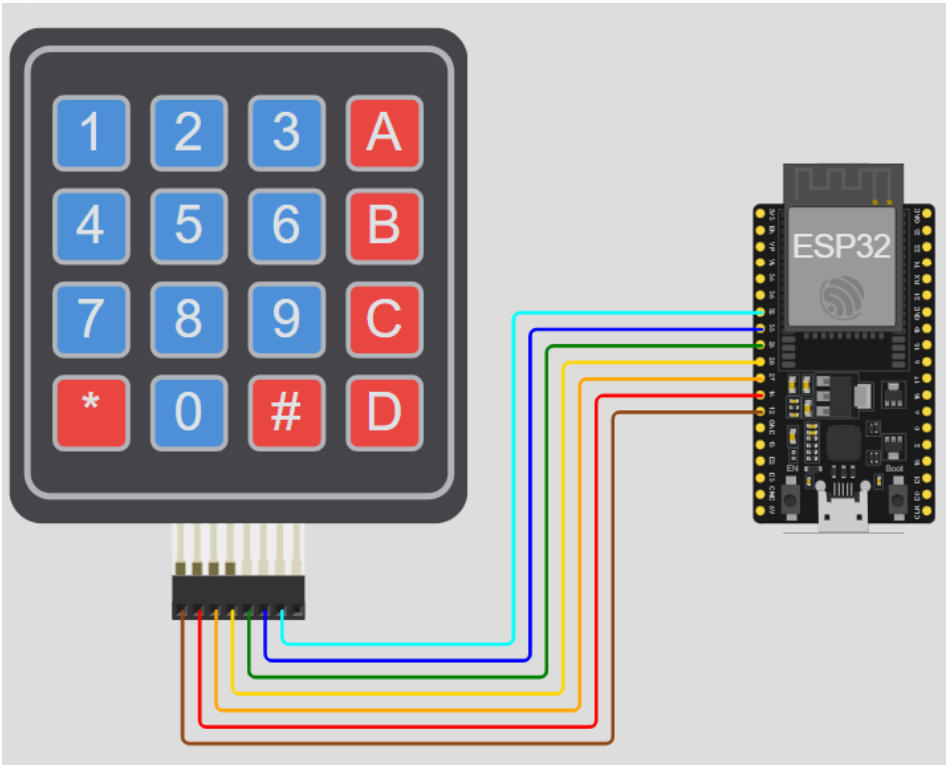


Figure 3.9: 4x3 Membrane Keypad Wiring

Keypad Pin	Connected ESP32 GPIO
Row 1 (R1)	GPIO12
Row 2 (R2)	GPIO14
Row 3 (R3)	GPIO27
Row 4 (R4)	GPIO26
Column 1 (C1)	GPIO25
Column 2 (C2)	GPIO33
Column 3 (C3)	GPIO32

Table 3.2: 4x3 Matrix Keypad Pin Connections to ESP32

3.2.4 Relay Module



Figure 3.10: Relay Module

The relay module is a commonly used single-channel electromechanical switch featuring the Songle **SRD-05VDC-SL-C** relay. It allows a low power control signal, typically from a microcontroller such as an ESP32, Arduino, or Raspberry Pi, to switch on or off a much higher power electrical circuit [14]. This provides electrical isolation between the control circuit and the load, thereby protecting sensitive components Figure 3.10.

The core of the module is the blue Songle relay Figure 3.11, which contains an electromagnet and switch contacts. Input pins include:



Figure 3.11: Songle Relay Module

- **VCC**: Connected to a 5V DC power source.
- **GND**: Connected to the ground.
- **IN**: Receives the digital signal to trigger the relay (usually LOW).

Output terminals (via screw terminal block) include:

- **COM (Common):** The central terminal.
- **NO (Normally Open):** Disconnected when idle; connected to COM when the relay is activated.
- **NC (Normally Closed):** Connected to COM when idle; disconnected when the relay is activated Figure 3.12.



Figure 3.12: Output Relay Module

When the IN pin receives the correct signal (typically LOW), a small current flows to activate an onboard transistor, energizing the relay coil. This generates a magnetic field that pulls the internal armature, switching the contacts—**disconnecting COM from NC** and **connecting COM to NO** [15].

- **Red LED:** Indicates the module is powered.
- **Green LED:** Lights up when the relay is actively switching Figure 3.13.

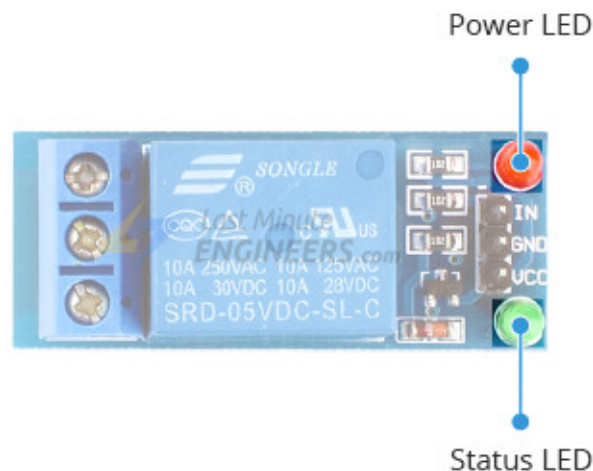


Figure 3.13: Indicator Relay Module

Supporting components include:

- A transistor to amplify the control signal.
- A flyback diode to protect the circuit from voltage spikes.
- Resistors for current limiting and signal control.

This module allows safe and reliable control of high-power devices such as lamps, fans, or household appliances while keeping control electronics fully isolated from the high-voltage side. In our access control system, we chose the relay because it allows us to safely control the electric door lock using low-power signals from a microcontroller. The relay provides electrical isolation between the control circuit and the high-voltage load, ensuring both the safety of the system and the protection of sensitive electronic components.



Figure 3.14: relay module pinout

Wiring Configuration of the Relay Module with ESP32 for Door Lock Control

In this configuration, the ESP32 microcontroller interfaces with a single-channel relay module to control an electric door lock. The control signal originates from GPIO pin 13 of the ESP32 and is directed through a protective circuit before reaching the relay. Specifically, the signal first passes through a diode (1N4007) to prevent reverse current, followed by a 1 (k Ω) resistor to limit current. This line then connects to the base of an NPN transistor (2N2222), which acts as a signal amplifier and isolator [16]. The emitter of the 2N2222 transistor is connected to ground (GND), while the collector is connected to the IN pin of the relay module. This arrangement allows the low-power GPIO signal from the ESP32 to switch the transistor, which in turn controls the relay input using current from the VCC supply. The relay module itself is powered by the 5V output from the ESP32, and both devices share the same ground (0V reference) to ensure circuit stability. On the relay output side, the common terminals (COM) and normally open terminals (NO) are used to control the electric door lock. In its default (inactive) state, the relay leaves the COM-NO path open, keeping the door locked. When the relay is activated via the transistor, the internal switch closes the COM-NO connection, supplying power to the door lock and unlocking it. This configuration provides multiple layers of protection and control: the diode protects the GPIO pin, the resistor controls the base current of the transistor, and the transistor itself isolates and amplifies the signal. Furthermore, using the relay offers electrical isolation between the low-voltage control circuit of the ESP32 and the higher-voltage load (door lock), ensuring the safety and reliability of the entire system (Figure 3.15).

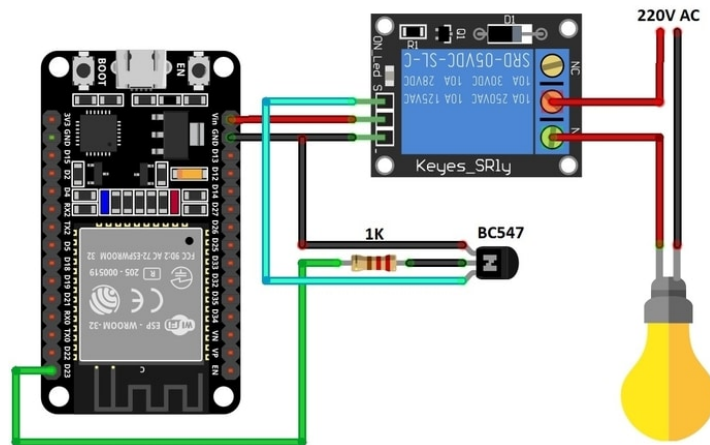


Figure 3.15: Wiring Relay Module to ESP32

Electric Door Lock

An electric door lock is a type of locking mechanism that operates using electrical power to control the locking and unlocking of a door. It is widely used in access control systems for residential, commercial, and industrial security applications. The lock shown in the image is a stainless steel electric strike lock that combines both electronic and mechanical access. It can be remotely activated by a microcontroller (such as ESP32) through a relay module [17]. This type of lock typically operates on 12V DC and consumes about 1 to 2 amps when activated. It remains locked when power is off (fail-secure configuration), which ensures safety by preventing unauthorized access in the event of a power failure unless the manual key is used. One of the primary reasons for choosing this type of lock is its electrical control integration; it can be easily managed by a relay connected to an ESP32-based system, enabling remote or automated unlocking when access is granted. It also provides high security due to its strong and durable lock body, making it suitable for environments that require reliable physical protection. Additionally, the lock offers dual access—electronic and manual—by including a mechanical keyhole that ensures entry is possible during emergencies such as power outages or system failures. The fail-secure design ensures the lock remains closed when unpowered, adding an extra layer of security during electrical disruptions. In summary, this electric door lock offers a balanced combination of security, automation, and safety, making it an ideal choice for our access control project (Figure 3.16).



Figure 3.16: door lock

3.2.5 Buzzer

Buzzer: A buzzer is an acoustical signaling device that emits sound upon the application of an electric current. It is used comprehensively in electronic circuits to offer audible warning, indication, or alerts. Buzzers are generally categorized into two types: active buzzers, with an internal oscillator and emitting sound upon the application of a DC voltage, and passive buzzers, requiring an external source, usually a PWM signal from a microcontroller, to make sound Figure 3.17.



Figure 3.17: Buzzer

Functionally, as voltage is passed through the buzzer, a diaphragm or piezoelectric component within the device vibrates and generates audible sound waves. The frequency and modulation of the input signal determine the pitch and pattern of the resulting sound. In our access control system, immediate auditory feedback is provided by the buzzer, beeping momentarily for a right or wrong identification of a fingerprint, thereby informing the user of access granted or denied. This allows simple and real-time interaction without the need for a visual interface. The buzzer was chosen for implementation in our system due to some significant advantages: it provides instant audio feedback that adds value to the user experience, low power consumption—making it a good fit for embedded applications—small form factor that makes it convenient to fit into the PCB’s design, and simple interfacing with microcontrollers such as the ESP32. In all, the buzzer serves to make the access control system more responsive and more user-friendly by providing clear audible status feedback without sacrificing the effectiveness and simplicity of the system.

Buzzer Wiring to ESP32

In our access control system, the buzzer is connected to GPIO pin 4 of the ESP32. One terminal of the buzzer is connected directly to this pin to serve as a digital output for sound activation, while the other terminal is connected to the ground (GND) of the board. This configuration allows the ESP32 to send a digital signal to activate the buzzer as needed Figure 3.18.

To enhance user experience and provide immediate feedback, two distinct sound patterns are used: a short single tone to indicate successful fingerprint recognition, and a fast double tone or a tone with a different pitch to indicate access denial. These different sounds are generated by controlling the timing and frequency of the signal sent to the buzzer using PWM (Pulse Width Modulation), which clearly distinguishes between different state of the system and offers an effective and intuitive auditory communication method.

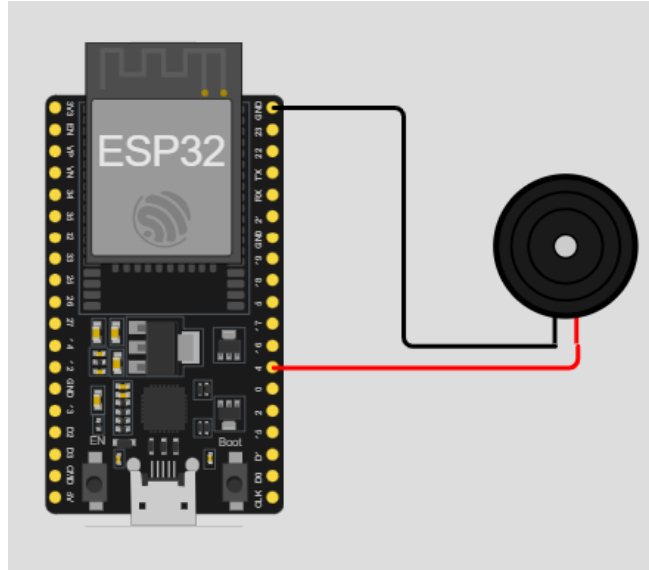


Figure 3.18: Buzzer Wiring to ESP32

3.2.6 Power Supply Design

The power architecture of the access control system is built around a 12V 2A DC charger, which acts as the main power source for all components. This setup is designed to efficiently meet the different voltage requirements of the system, particularly the ESP32 microcontroller and the electric door lock.



Figure 3.19: charger 12V

To power the ESP32, which operates at 3.3V internally but can be supplied via a regulated 5V input, a linear voltage regulator (LM7805) is used. The LM7805 takes the 12V input and regulates it down to a stable 5V output, which is then connected to the 5V pin of the ESP32. This ensures that the ESP32 receives clean and safe power without the risk of overvoltage, which could otherwise damage the board.

12 V to 5 V Converter

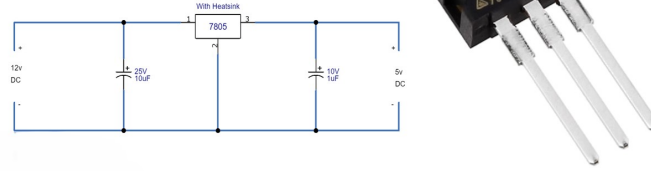


Figure 3.20: LM7805

In parallel, the same 12V line is directly connected to the electric door lock, which is rated for 12V operation. The door lock uses this voltage to energize its internal electromagnet, allowing it to unlock when activated. This direct connection avoids the need for a separate power supply and simplifies the layout of the system. To further enhance safety and efficiency, the ground (GND) of all components is tied to a common reference, ensuring stable operation and signal integrity throughout the system. The use of the LM7805 voltage regulator provides electrical isolation between the high-voltage (12V) and low-voltage (5V) sections, protecting sensitive components such as the ESP32 (Figure 3.20). The chosen 12V, 2A capacity ensures that both the lock and the regulator can operate without voltage drops or overheating during activation. This power design provides a reliable, centralized power solution for both control logic and actuation, ensuring that the system remains compact and cost-effective while maintaining proper electrical isolation and protection.

3.3 System Schematic

This section provides a comprehensive overview of the complete hardware schematic of the access control system. The schematic serves as a detailed blueprint for the physical implementation of the system, illustrating the interconnections between all major components and highlighting their respective roles within the architecture. The design integrates the ESP32 microcontroller, which acts as the central processing unit, coordinating all input and output operations. It interfaces with several peripheral devices, including the fingerprint sensor (for biometric identification), a 4x3 matrix keypad (for numeric code entry), a buzzer (for audible feedback), and a single-channel relay module (for controlling the electronic door lock). To manage the system's power requirements, a 12V, 2A DC power supply is used. Power is distributed via a voltage regulator (LM7805), which reduces the voltage to 5V to safely power the ESP32 and other 5V-tolerant components, while the 12V line directly energizes the electronic lock. Proper ground referencing is maintained throughout the circuit to ensure electrical stability and noise immunity. The schematic diagram clearly shows all the wiring connections, power supply lines, signal flow paths, and protective components such as diodes and resistors used for current limiting and reverse polarity protection. This systematic representation not only supports accurate hardware assembly but also facilitates troubleshooting, future upgrades, and documentation of the system design. Following this schematic, developers and technicians can precisely reproduce the physical circuit, ensuring reliable performance and operational safety of the access control system (Figure 3.21).

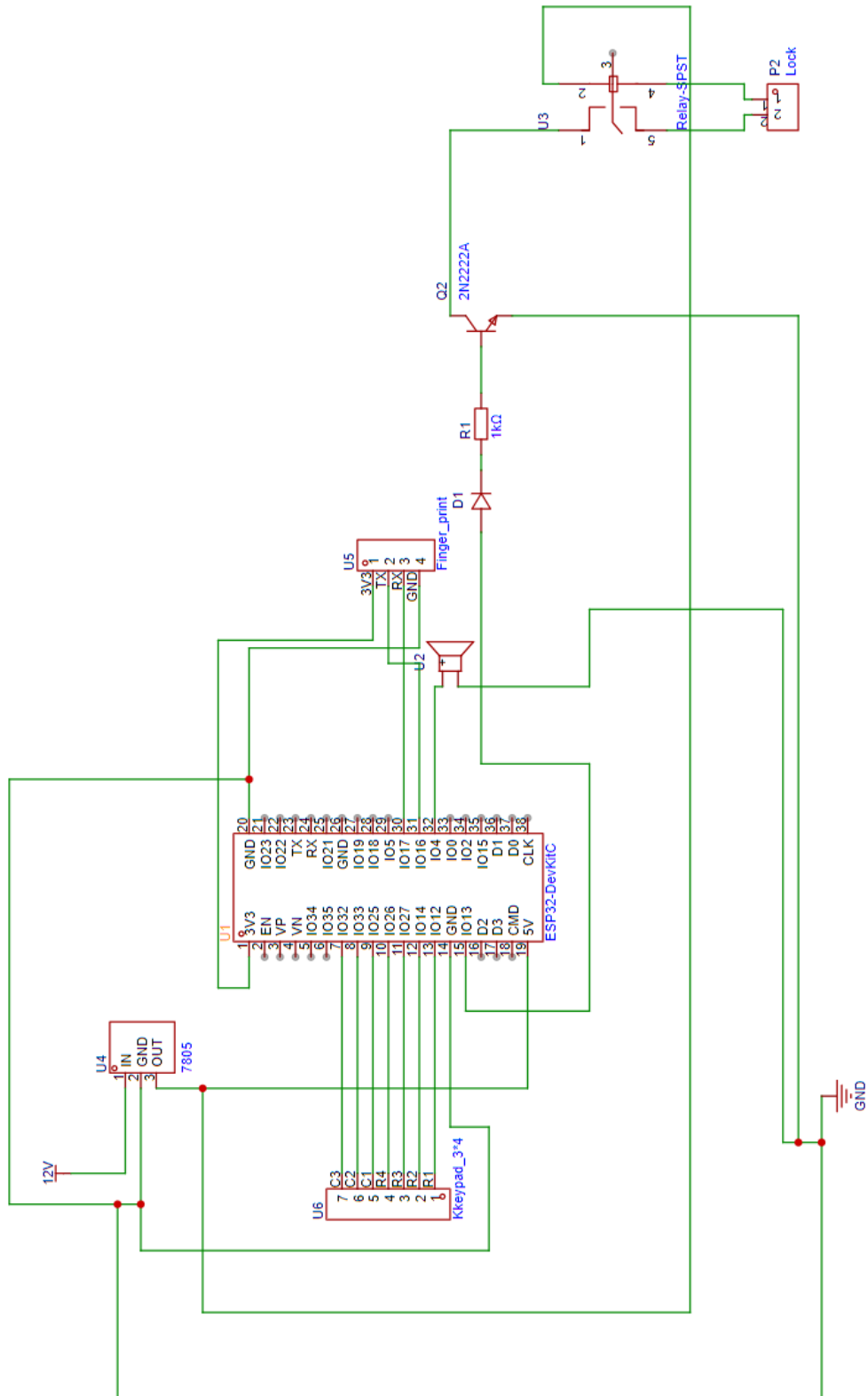


Figure 3.21: Complete System Hardware Schematic

3.3.1 Circuit Schematic and Component Analysis

EasyEDA is a comprehensive web-based electronic design automation (EDA) platform that provides integrated tools for schematic capture, PCB layout design, and circuit simulation. This cloud-based platform enables engineers and hobbyists to design, simulate, and share electronic circuits collaboratively without requiring local software installation, offering extensive component libraries and real-time design verification capabilities. The presented schematic illustrates a sophisticated embedded system centered around an ESP32 development board (ESP32-DevKitC), implementing a security or access control system with biometric authentication capabilities. The circuit operates on a 12V power supply that is regulated down to the ESP32's required voltage levels through a 7805 voltage regulator (U4). The regulator's input pin connects to the 12V supply rail, with its ground pin connected to the common ground plane, and its output pin providing regulated 5V power to the system components. The ESP32 microcontroller serves as the central processing unit, with its GPIO pins strategically allocated for various interface functions. The keypad interface (U6) represents a 4x3 matrix keypad connected to the ESP32 through digital pins, enabling numeric input for security codes or system commands. The keypad matrix configuration includes keys arranged as '1','2','3' in the first row, '4','5','6' in the second row, '7','8','9' in the third row, and '*', '0', '#' in the fourth row. The keypad's row pins are connected to GPIO12 (R1), GPIO14 (R2), GPIO27 (R3), and GPIO26 (R4), while the column pins connect to GPIO25 (C1), GPIO33 (C2), and GPIO32 (C3), allowing for efficient key scanning through multiplexing techniques. A critical component in this system is the fingerprint sensor module (U5), which connects to the ESP32 via UART communication protocol. The sensor's VCC pin receives 3.3V power, its TX and RX pins connect to corresponding GPIO pins TX to GPIO16 and RX to GPIO17 on the ESP32 for serial data transmission, and its ground pin connects to the common ground plane. This biometric sensor enables the system to capture, process, and authenticate fingerprint data for secure access control. The circuit incorporates a transistor-based switching mechanism using Q2 (2N2222A NPN transistor) to control a relay module (U3). The transistor's base connects to GPIO pin 13 on the ESP32 through a current-limiting resistor R1 (1 k Ω), while its collector connects to the relay's control input and its emitter connects to ground. Additionally, the system includes an audio feedback component through a buzzer connected to GPIO pin 4, providing audible notifications for user interactions and system status. This configuration allows the ESP32 to control high-power loads through the relay's normally open and common terminals, which are brought out to connection points for external device control. The relay module (Relay-SPST) features standard connections including power supply pins (5V and ground), control input from the transistor circuit, and switching contacts (common, normally open, and normally closed) accessible through terminal connections P2. This relay configuration enables the system to control external devices such as electric locks, alarms, or other security mechanisms. Power distribution throughout the circuit follows a hierarchical approach, with the 12V input supply feeding the voltage regulator, which then provides stable power to the ESP32 and associated components. Ground connections are unified through a common ground plane, ensuring proper reference levels for all circuit components. The schematic demonstrates careful consideration of power requirements, signal routing, and component interfacing necessary for a functional embedded security system with multiple input modalities and output control capabilities.

3.4 Dual Authentication System Code

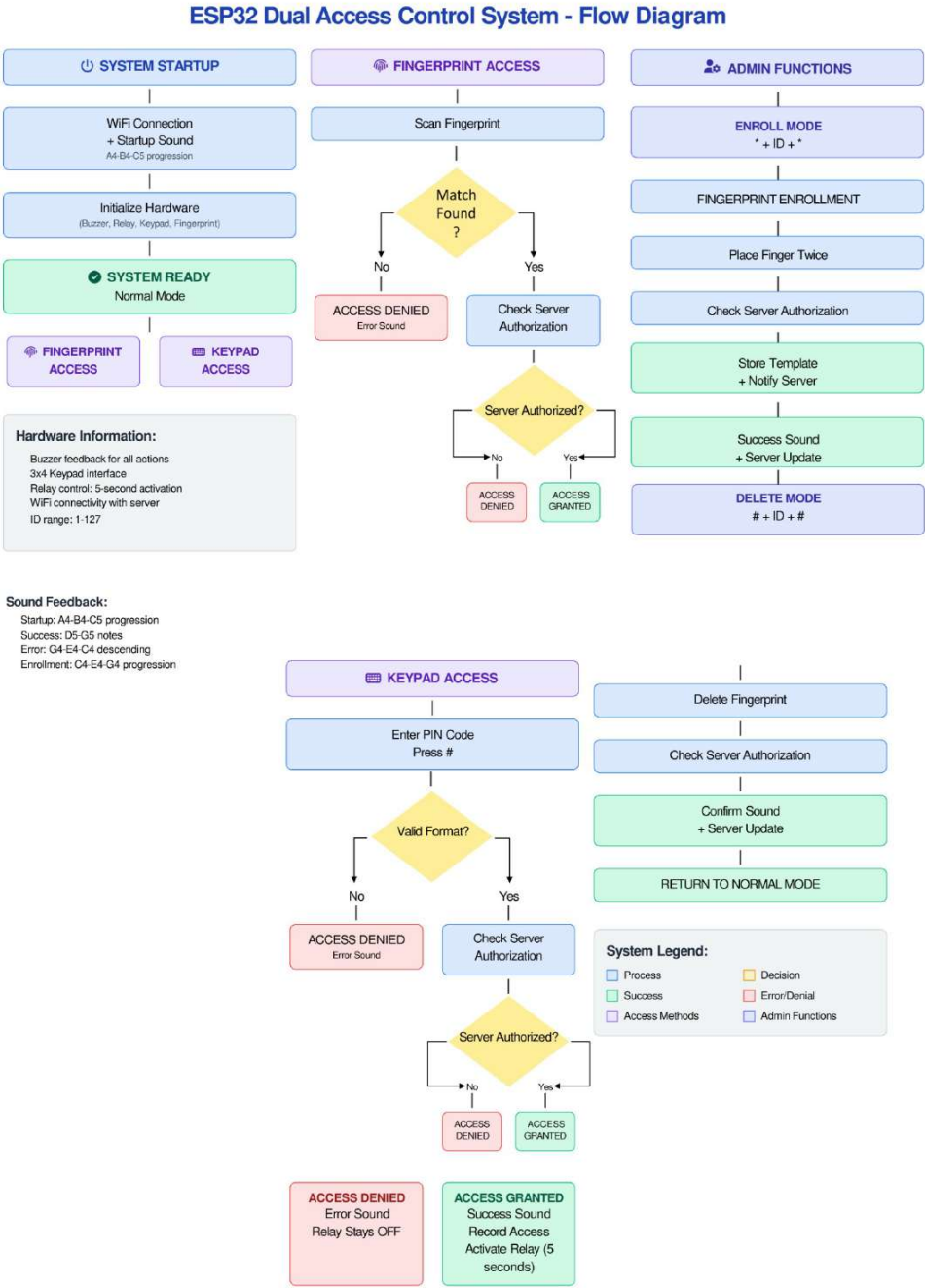


Figure 3.22: Organigram of Access Control System

3.5 Conclusion

In this chapter, we focused on the design and implementation of the hardware layer of the access control system, centered around the ESP32 microcontroller. The system combines biometric identification via the AS608 fingerprint sensor, PIN-based input through a 4x3 keypad, and door control using a relay and buzzer for real-time feedback. The ESP32 also connects to a Wi-Fi network to ensure synchronization with the backend server.

This part demonstrates the ESP32's ability to independently manage local authentication, execute immediate hardware actions, and support user enrollment and deletion. While the ESP32 handles real-time decision-making at the access point, its true strength lies in its integration with the central server, which enables data consistency, attendance tracking, and remote system management. This collaboration between embedded and backend components forms the foundation for a scalable and intelligent access control solution, leading to the next chapter, which details the server-side architecture.

Chapter 4

Software Design for Secure Access Control

4.1 Introduction

This chapter delves into the technical software design and implementation of the proposed intelligent lab access control system. The software component is the most important part, integrating the system's critical functions so that it runs securely, reliably, and efficiently. It encompasses both low-level communication with physical hardware and high-level management and monitoring capabilities. This chapter is structured to introduce in depth the two principal software elements: the embedded system's firmware, which is responsible for real-time control and communication with input/output devices, and the backend server, which is responsible for centralized data management, remote monitoring, and API services. These two elements together form a robust and comprehensive framework that unifies hardware-level access control with sophisticated data processing and administrative management. The following sections will discuss the design philosophy, implementation methods, and the intricate communication interfaces on which these primary components communicate without any interruption and produce a fully functional and manageable access control system.

Software Overview: This chapter presents the software architecture and implementation details of the proposed access control system. The software component plays a critical role in ensuring secure, reliable, [18] and efficient operation of the system by handling both hardware interaction and data management functionalities. The chapter is divided into two primary sections corresponding to the two main components of the system: the embedded system and the back-end server.

- **Embedded System:** This component is responsible for interacting with hardware components. This includes programming the **ESP32** microcontroller [8] to control and communicate with input and output devices such as the fingerprint sensor, keypad, and electronic lock. This module performs real-time processing and decision-making based on user input and authentication procedures.
- **Back-end System:** A monitoring and management system developed using **Python**, which enables remote access supervision and centralized log storage.

Together, these two components form a cohesive and secure access control framework that integrates hardware-level control with centralized data processing and management. The following sections detail the design, implementation, and interaction between these components.

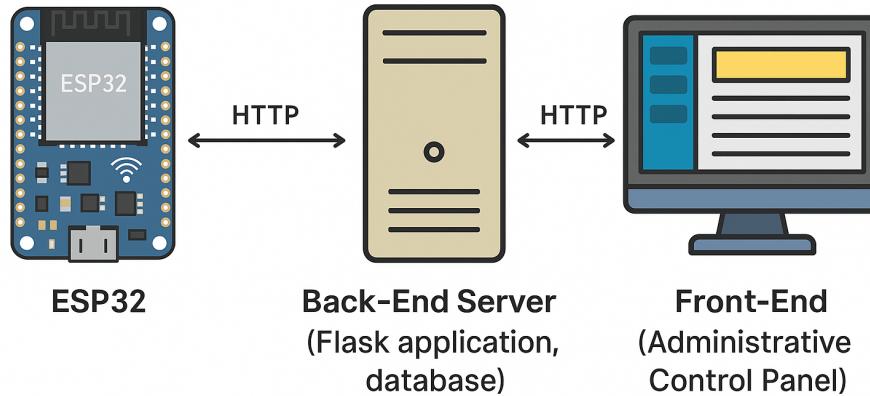


Figure 4.1: Diagram of Connection Softwares

4.2 Programming the ESP32 Unit

The ESP32 firmware was developed to achieve the following objectives:

1. **User Fingerprint Acquisition:** The ESP32 communicates with a biometric fingerprint sensor to capture the fingerprints of users attempting to access the system. This requires initialization and configuration of the sensor, as well as capturing and preprocessing the fingerprint templates for matching.
2. **PIN Code Entry via Keypad:** A matrix keypad is integrated into the system to allow users to enter a personal identification number (PIN). The ESP32 continuously listens for key presses [19], decodes the input sequence, and temporarily stores it for verification.
3. **Remote Data Matching:** Once the fingerprint and/or PIN code is received, the ESP32 performs authentication by comparing the provided data against the data stored in the remote server for validation. This involves sending requests to the backend `/api/check_access` endpoint (??)
4. **Access Decision and Lock Control:** Based on the result of the authentication process, the ESP32 decides whether to grant or deny access. If access is granted, the ESP32 triggers a digital output to unlock the electronic door lock. If access is denied, appropriate feedback (e.g., sound or LED alert) is provided to the user.
5. **Event Logging and Reporting:** Every access attempt—whether successful or failed—is logged by the ESP32 and sent to the central monitoring server via the `/api/check_access` API [8]. The report includes information such as timestamp, method of authentication, and result status, ensuring traceability and aiding system audits ??.

The following diagram Figure 4.2 illustrates the operational flow of the ESP32 authentication process.

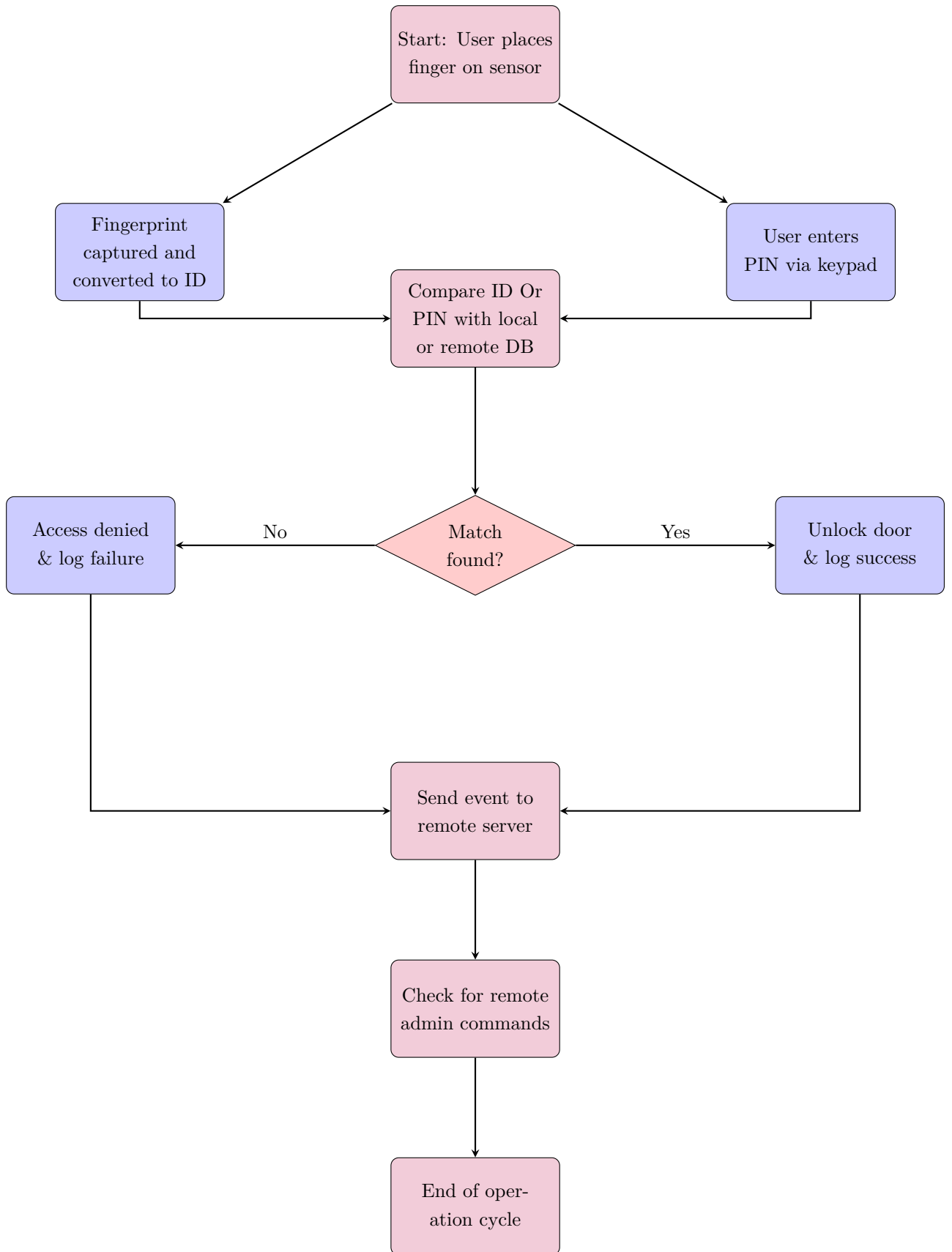


Figure 4.2: Flowchart of the ESP32 Authentication and Access Control Process

6. **Remote Command Handling:** The ESP32 is also designed to receive remote commands from the back-end server [8]. For example, an administrator may remotely unlock the door in case of an emergency or maintenance scenario. Secure communication protocols are used to ensure that only authorized commands are executed. This can be facilitated by the ESP32 periodically polling the server for commands or by implementing a push notification mechanism.

This modular approach to ESP32 programming ensures that the system is not only robust and autonomous in normal operation but also responsive to centralized management when needed.

4.2.1 Operating Mechanism

The ESP32 unit is programmed to execute a well-defined sequence of operations to manage access control securely and efficiently. The overall workflow involves user authentication, access decision-making, logging, and remote command handling. The following outlines the operational mechanism in detail:

1. **Fingerprint Acquisition and Identification:** When a user places their finger on the fingerprint sensor, the sensor captures the fingerprint image and extracts a set of unique biometric features. These features are then converted into a unique identification number (ID), which is used for comparison against stored templates.
2. **PIN Code Input via Keypad:** Following successful fingerprint scanning (or as an alternative method), the system allows the user to enter a secret PIN code using the keypad [20]. The ESP32 reads the sequence of digits entered by the user and temporarily stores it for verification.
3. **Authentication and Verification:** The system performs authentication by validating either the fingerprint ID or the entered PIN code. This verification is primarily conducted remotely by forwarding the data to the central server's `/api/check_access` endpoint for real-time verification against the comprehensive user database `??`. The server's response dictates the access decision.
4. **Access Decision and Physical Control:** Upon receiving the authentication result from the server, the ESP32 unit takes the appropriate action. If access is granted, it activates the electronic lock, allowing entry. Concurrently, visual (LEDs) and auditory (buzzer) feedback is provided to the user. If access is denied, the lock remains engaged, and distinct feedback is given to indicate the refusal.
5. **Event Logging and Reporting:** Each authentication attempt, regardless of its outcome, is logged locally on the ESP32 (temporarily, if needed) and immediately transmitted to the central monitoring server via the `/api/check_access` API. The event log includes details such as timestamp, user ID (if identified), authentication method, and result (success or failure). This ensures full traceability and allows administrators to audit access activities `??`.
6. **Remote Command Execution and Synchronization:** In addition to autonomous operation, the ESP32 periodically polls the backend's `/api/get_active_users/<lab_unique_id>` endpoint to fetch updated lists of authorized users and their credentials (codes and fingerprint IDs) `??`. This ensures that the ESP32's local cache of authorized users is always synchronized with the central database. The ESP32 is also designed to listen for specific remote commands issued by the system administrator via the back-end interface, such as remote door unlocking for emergencies or maintenance. All remote interactions are secured to prevent unauthorized access.

This structured mechanism ensures that the system operates autonomously while maintaining connectivity with the central server for monitoring and administrative control.

4.3 Back-end System

The software component consists of an integrated web system built using the **Flask** framework in **Python**, providing an administrative interface for comprehensive control. The backend forms the core of the system, processing business logic, managing interactions with the database Figure 4.3, and providing the necessary **endpoints** for communication between devices and the frontend. The backend primarily relies on the `app24.py` and `config.py` files and .

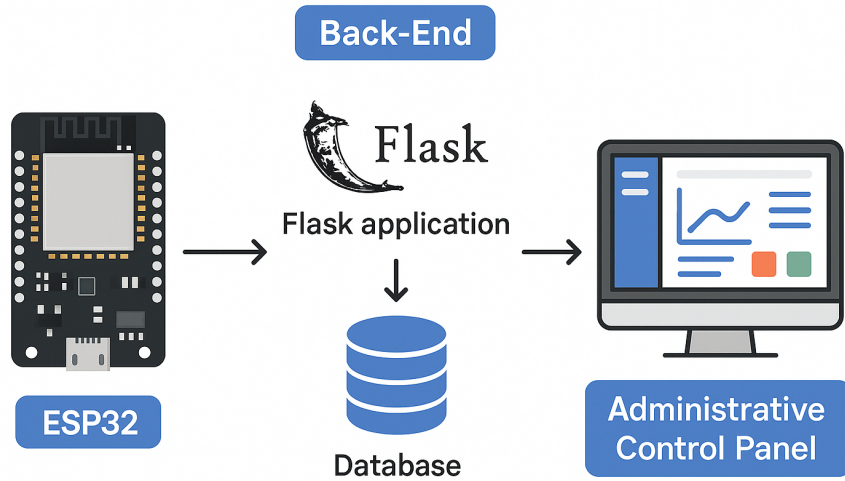


Figure 4.3: Diagram Back End Server

4.3.1 Flask Framework

Flask is a lightweight and minimalistic web framework built in **Python**. In this project, it is used to build the web application that provides both the administrative interface and the **APIs** [7]. **Flask** is characterized by its flexibility and ease of use, making it suitable for web applications that require precise control over components.

- **Route Definition:** Flask allows defining different URL routes which are linked to specific **Python** functions. For example, the `/api/check_access` route in `app24.py` handles access verification requests from ESP32 devices.
- **Request Handling:** Flask provides powerful tools for processing incoming HTTP requests (**GET**, **POST**) and extracting data from them (e.g., `request.get_json()` or `request.form.get()`).
- **Template Rendering:** `render_template()` is used to render dynamic HTML pages (such as `index23.html` and `login.html`), where data can be passed from the backend to the templates.

4.3.2 User Management and Authentication (Flask-Login)

To ensure the security of the administrative interface, the **Flask-Login** extension is used to manage administrator (**AdminUser**) login sessions and protect routes that require administrative privileges [21].

- **Session Management:** **Flask-Login** facilitates user login and logout processes and manages their sessions via **cookies**.

- **Route Protection:** The `@login_required` decorator (and the custom `@admin_required` decorator in `app24.py`) is used to restrict access to specific routes so that they can only be accessed by authenticated users (and administrators in our case).
- **Current User Object:** Provides easy access to information about the currently logged-in user via the `current_user` object.
- **User Loader:** The `load_user()` function is used to define how a user object is loaded from the user ID stored in the session. In this project, the static `AdminUser` object is loaded.

4.3.3 Database (SQLAlchemy)

SQLAlchemy is used as a powerful Object Relational Mapper (ORM) layer for interacting with the relational database. SQLAlchemy allows interaction with the database using Python objects instead of writing direct SQL queries [6], which simplifies the application development process and improves maintainability. The project supports SQLite by default (for development) and can be easily configured to work with DATABASE_URL environment variable.

- **Model Definition:** Data models are defined as Python classes that represent tables in the database, and their properties (`columns`) and relationships are defined. The main models in this project are:

1. Lab:

- **Purpose:** To store information about the laboratories available in the system.
- **Properties:**
 - * `id`: Unique primary key for the lab.
 - * `name`: Name of the lab (unique).
 - * `unique_id`: Unique identifier for the lab used for communication with ESP32 devices (unique).
 - * `logs`: A relationship with access logs (`AccessLog`), pointing to logs associated with this lab.

2. User:

- **Purpose:** To store data for users who are allowed access to the labs.
- **Properties:**
 - * `id`: Unique primary key for the user.
 - * `name`: User's name.
 - * `user_code`: User's secret code (for keypad access, unique, optional).
 - * `fingerprint_id`: User's fingerprint ID (for fingerprint reader access, unique, optional).
 - * `is_active`: User status (active/inactive), determines if they are allowed access.
 - * `logs`: Relationship with access logs (`AccessLog`), pointing to logs associated with this user.
 - * `allowed_labs`: A many-to-many relationship with the Lab model via the `user_lab_permissions` intermediary table, defining the labs the user is allowed to access.

3. AccessLog:

- **Purpose:** To record every access attempt to the labs, whether successful or failed.
- **Properties:**

- * **id**: Unique primary key for the log entry.
- * **timestamp**: Timestamp of the access attempt.
- * **user_id**: Foreign key pointing to the user who attempted access (can be NULL if the user is unknown).
- * **lab_id**: Foreign key pointing to the lab that was attempted to be accessed (can be NULL if the lab is unknown).
- * **user_name**: Name of the user at the time of the access attempt (for historical records).
- * **lab_name**: Name of the lab at the time of the access attempt (for historical records).
- * **access_method**: Access method used (e.g., **keypad** or **fingerprint**).
- * **status**: Status of the access attempt (e.g., **granted**, **denied**, **denied (permission)**, **error**).

4. **user_lab_permissions**:

- **Purpose**: An intermediary table used to manage the many-to-many relationship between users and labs. This table records which users are allowed access to which labs.
- **Properties**:
 - * **user_id**: Foreign key pointing to the user ID.
 - * **lab_id**: Foreign key pointing to the lab ID.

- **Table Creation (`create_tables()`)**: The `create_tables()` function in `app24.py` is used to create all tables defined by SQLAlchemy in the database upon application startup, ensuring the data infrastructure is ready.

4.4 Frontend (User Interface)

The frontend of the system provides an intuitive and interactive web interface for administrators to manage the access control system remotely. It is built using standard web technologies: **HTML** for structure, **Tailwind CSS** for styling, and **JavaScript** for dynamic behavior [22]. The core frontend components are the Administrative Dashboard (`index23.html`), the Login Page (`login.html`), and the associated styling (`index23.css`).

4.4.1 Administrative Dashboard (`index23.html`):

The Administrative Dashboard serves as the central control panel for system administrators. It is designed to be responsive and user-friendly, allowing for efficient management of users, laboratories, and access logs. The dashboard's layout and styling are handled by **Tailwind CSS**, ensuring a modern and clean appearance across various devices [cite: `index23.html`, `index23.css`].

User Management

This section of the dashboard provides comprehensive tools for managing system users the following figure showing that Figure 4.4:

- **User Listing**: Displays a clear list of all registered users, including their names, activation status, user codes (if assigned), and fingerprint IDs (if assigned).
- **Add New User**: Administrators can add new users by providing a name, an optional user code (for keypad access), and an optional fingerprint ID (for biometric access). Input validation is performed on the backend to ensure data integrity [cite: `app24.py`].

Users

Add User

Add New User

Name

User Code (Optional)

Fingerprint ID (Optional)

Add User

NAME	STATUS	ACTIONS
<div>OMAR</div> <div>Code: 1234</div> <div>LAB AUOT</div> <div>Default Lab</div>	Inactive	<div>Activate</div> <div>Select Lab</div> <div>Add</div> <div>Delete</div>
<div>ahmed</div> <div>Code: 12333</div> <div>Default Lab</div>	Active	<div>Deactivate</div> <div>Select Lab</div> <div>Add</div> <div>Delete</div>

Figure 4.4: User Management With Features

- **Activate/Deactivate Users:** The system allows administrators to toggle the active status of users. Deactivating a user immediately revokes their access privileges without deleting their record, providing flexibility for temporary suspensions or inactive accounts.
- **Delete Users:** Administrators have the ability to permanently delete user records from the system. This action also cascades to remove associated access logs and lab permissions, ensuring data consistency. A confirmation prompt is used to prevent accidental deletions.
- **Lab Permissions Management:** For each user, the dashboard displays the laboratories they currently have access to. Administrators can grant or revoke access to specific labs through a simple interface, ensuring granular control over user permissions.

Laboratory Management

This section enables administrators to manage the laboratories within the system as shown in the figure below Figure 4.5:

Labs

Add Lab

Add New Lab

Lab Name

Unique ID

Only letters, numbers, underscores, and hyphens

Add Lab

NAME	ID	ACTIONS
Default Lab	LAB001	Delete
LAB AUOT	LAB-AUOT	Delete

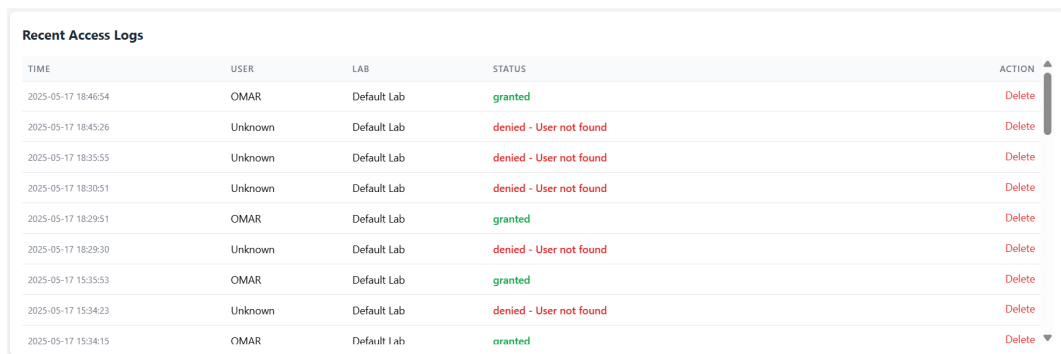
Figure 4.5: Laboratory Management With Features

- **Lab Listing:** Displays a list of all registered laboratories, including their names and unique identifiers.

- **Add New Lab:** Administrators can add new laboratories by providing a unique name and a unique ID. The unique ID is crucial for the ESP32 units to identify the specific lab they are installed in. Backend validation ensures the uniqueness and format of these IDs.
- **Delete Labs:** Administrators can delete laboratory records. Deleting a lab also removes all associated access logs and revokes access permissions for that lab from all users, maintaining database integrity. A confirmation prompt is used for this critical action.

Access Log Display:

The dashboard provides a real-time view of all access attempts, offering critical insights into system activity Figure 4.6 :



TIME	USER	LAB	STATUS	ACTION
2025-05-17 18:46:54	OMAR	Default Lab	granted	Delete
2025-05-17 18:45:26	Unknown	Default Lab	denied - User not found	Delete
2025-05-17 18:35:55	Unknown	Default Lab	denied - User not found	Delete
2025-05-17 18:30:51	Unknown	Default Lab	denied - User not found	Delete
2025-05-17 18:29:51	OMAR	Default Lab	granted	Delete
2025-05-17 18:29:30	Unknown	Default Lab	denied - User not found	Delete
2025-05-17 15:35:53	OMAR	Default Lab	granted	Delete
2025-05-17 15:34:23	Unknown	Default Lab	denied - User not found	Delete
2025-05-17 15:34:15	OMAR	Default Lab	granted	Delete

Figure 4.6: Access Log Control

- **Detailed Log Entries:** Displays a table of recent access logs, including the timestamp of the attempt, the user involved (or "Unknown" if not identified), the laboratory name, the access method used (e.g., keypad, fingerprint), and the status of the attempt (e.g., "granted", "denied", "denied (permission)", "error") Figure 4.6
- **Dynamic Updates (Polling):** The logs are dynamically updated using a polling mechanism. A JavaScript function in `index23.html` periodically fetches data from the backend's `/api/data_status` endpoint [cite: index23.html]. If changes are detected in the log, user, or lab data (e.g., new log entries, user additions/deletions, lab changes), the page automatically reloads to display the most current information [6]. This ensures that administrators always have an up-to-date view of system activity without manual refreshing.

4.4.2 Login Page (`login.html`)

The Login Page provides a secure gateway for administrators to access the system's administrative functions Figure 4.7.

- **Secure Authentication:** Administrators enter their username and password to gain access. The backend handles authentication using `Flask-Login` [cite: app24.py, login.html].
- **Remember Me Option:** A "Remember me" checkbox allows administrators to maintain their login session across browser sessions, enhancing convenience.
- **Show Password Functionality:** A JavaScript function is implemented to toggle the visibility of the password input field, improving user experience and reducing input errors [cite: login.html].

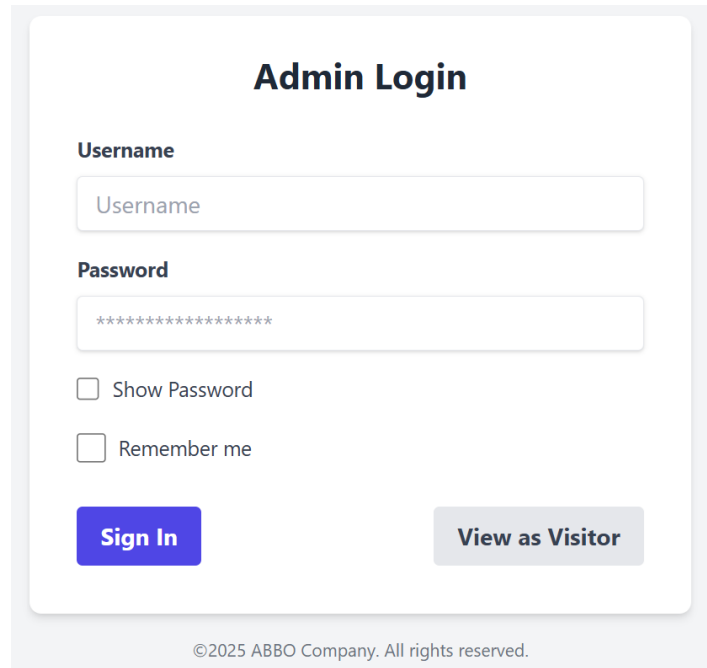
The image shows a web form titled "Admin Login". It has two input fields: "Username" and "Password". The "Username" field contains the text "Username". The "Password" field contains a series of asterisks "*****". Below the password field are two checkboxes: "Show Password" and "Remember me". At the bottom of the form are two buttons: "Sign In" (a solid blue button) and "View as Visitor" (a light gray button). Below the buttons, there is a copyright notice: "©2025 ABBO Company. All rights reserved." The entire form is enclosed in a light gray border.

Figure 4.7: Admin Login Page

- **Visitor View:** A link is provided to allow users to view the dashboard as a visitor without administrative privileges, offering a public view of the system’s status (e.g., logs, but without management actions).

4.4.3 Flash Messages (`index23.css`)

The system incorporates a robust flash messaging system to provide immediate and contextual feedback to the user on the frontend. These messages are rendered dynamically by Flask and styled using dedicated CSS classes [cite: `app24.py`, `index23.html`, `login.html`, `index23.css`].

- **Purpose:** To inform administrators about the success or failure of their actions (e.g., "User added successfully," "Invalid username or password," "Error deleting lab"), or to provide important informational messages.
- **Categorization:** Messages are categorized (e.g., `success`, `error`, `warning`, `info`), allowing for distinct visual styling (colors, borders) based on the message type, enhancing clarity and user comprehension.
- **Implementation:** Flask’s `flash()` function is used in the backend to store messages, which are then retrieved and displayed in the frontend using `get_flashed_messages()` within the HTML templates. Custom CSS rules in `index23.css` define the appearance of each message category.

4.5 Conclusion

In this chapter, we explored the software architecture of the intelligent access control system, emphasizing the synergy between the embedded ESP32 firmware and the centralized backend server. The ESP32 was shown to manage real-time biometric and keypad-based authentication, while also ensuring continuous communication with the server for logging and synchronization.

On the backend, the system—built with Flask and SQLAlchemy—provides a robust infrastructure for user management, permission control, and data persistence. The use of secure APIs, time zone-aware logging, and error handling mechanisms ensures reliability and auditability. Together, these software components form a scalable, secure, and remotely manageable system that meets the operational and administrative needs of modern laboratory environments.

General Conclusion

This project set out to address the pressing need for a modern, intelligent access control solution tailored to laboratory environments within academic institutions, where security, traceability, and usability are paramount. Beginning with a theoretical overview of Access Management Systems (AMS), we highlighted the evolution from traditional mechanical solutions to smart systems empowered by the Internet of Things (IoT), biometrics, and centralized data infrastructures. A deep dive into the local context revealed operational limitations and underscored the motivation for an improved solution. Through a comprehensive analysis of human resources, financial constraints, and administrative challenges, a clear problem statement was established, framing the need for a secure, flexible, and scalable platform that could operate effectively in a dynamic and resource-sensitive environment.










The core of the work focused on the practical realization of this objective by combining embedded hardware and server-side software. The ESP32 microcontroller was utilized as the autonomous agent for biometric and keypad-based local verification, interfacing directly with relays, buzzers, and sensors. In parallel, a robust backend was developed using Flask and SQLAlchemy to manage authentication logic, user databases, access logs, and administrative interfaces. The system architecture emphasized real-time decision-making, secure synchronization, and remote operability. Together, these components created a cohesive, distributed access control platform capable of meeting both security and administrative demands. The implementation demonstrates not only the feasibility of integrating low-cost embedded systems with scalable web technologies but also the importance of thoughtful system design that considers future extensibility, user convenience, and institutional needs. Ultimately, this project lays the groundwork for deploying intelligent access systems in other secure environments and opens the door for further enhancements such as mobile integration, AI-based analytics, and adaptive security policies.

Bibliography

- [1] Vincent C Hu, David Ferraiolo, D Richard Kuhn, et al. *Assessment of access control systems*. Vol. 76. US Department of Commerce, National Institute of Standards and Technology ..., 2006.
- [2] William Tolone et al. "Access control in collaborative systems". In: *ACM Computing Surveys (CSUR)* 37.1 (2005), pp. 29–41.
- [3] Melanie R Rieback, Bruno Crispo, and Andrew S Tanenbaum. "The evolution of RFID security". In: *IEEE Pervasive Computing* 5.01 (2006), pp. 62–69.
- [4] Vincent C Hu, David Ferraiolo, D Richard Kuhn, et al. *Assessment of access control systems*. Vol. 76. US Department of Commerce, National Institute of Standards and Technology ..., 2006.
- [5] Messaoud Benantar. *Access control systems: security, identity management and trust models*. Springer Science & Business Media, 2005.
- [6] Phillip Luong. "SQL with Python". In: (2020).
- [7] Fankar Armash Aslam, Hawa Nabeel Mohammed, and Prashant S Lokhande. "Efficient Way Of Web Development Using Python And Flask." In: *International Journal of Advanced Research in Computer Science* 6.2 (2015).
- [8] Vedat Ozan Oner. *Developing IoT Projects with ESP32: Automate your home or business with inexpensive Wi-Fi devices*. Packt Publishing Ltd, 2021.
- [9] Magdin Martin, Koprda Štefan, and Ferenczy L'ubor. "Biometrics authentication of fingerprint with using fingerprint reader and microcontroller Arduino". In: *Telkomnika (Telecommunication Computing Electronics and Control)* 16.2 (2018), pp. 755–765.
- [10] Zin Nwe Soe, AM Win, and DTH Thoung. "Implementation of Fingerprint based Student Attendance System with Notification by GSM Module". In: *International Journal of Science and Engineering Applications* 7.9 (2018), pp. 260–264.
- [11] Ammar Daniel Abd Rahman¹ and Ahmad Anwar Zainuddin. "Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology". In: *INTERNATIONAL GRAND INVENTION, INNOVATION AND DESIGN EXPO (IGIIDeation) 2025* (), p. 47.
- [12] Daniel Bhaskaran Raju. "Arduino based digital lasso lock security sytem using keypad". PhD thesis. 2022.
- [13] Shubham Thati. "Arduino Based Calculator". In: (2021).
- [14] Ariadna Calcines et al. "MOSAIC optical relay module: optical design, performance, and flexure analysis". In: *Ground-based and Airborne Instrumentation for Astronomy VII*. Vol. 10702. SPIE. 2018, pp. 3035–3047.
- [15] Deniz Gunduz et al. "The multiway relay channel". In: *IEEE Transactions on Information Theory* 59.1 (2012), pp. 51–63.

- [16] Yulianto Yulianto. “Relay Driver Based on Arduino UNO to Bridge the Gap of The Digital Output Voltage of The Node MCU ESP32”. In: *Engineering, Mathematics and Computer Science Journal (EMACS)* 5.3 (2023), pp. 129–135.
- [17] Karma Tshomo et al. “Dual door lock system using radio-frequency identification and fingerprint recognition”. In: *2019 IEEE 5th International conference for convergence in technology (I2CT)*. IEEE. 2019, pp. 1–5.
- [18] Junaid Mohammed et al. “Internet of Things: Remote patient monitoring using web services and cloud computing”. In: *2014 IEEE international conference on internet of things (IThings), and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCoM)*. IEEE. 2014, pp. 256–263.
- [19] R Padmasree, P Harshitha, and Shaik Muskan3 Anokya Kalwala. “Developing a Remote Access System by Interfacing ESP32 Microcontroller with 4X4 Keypad”. In: *International Journal* 11.10 (2023).
- [20] Ravi S Sandhu and Pierangela Samarati. “Access control: principle and practice”. In: *IEEE communications magazine* 32.9 (1994), pp. 40–48.
- [21] Gareth Dwyer, Shalabh Aggarwal, and Jack Stouffer. *Flask: building python web services*. Packt Publishing, 2017.
- [22] Mike McGrath. *HTML, CSS & JavaScript in easy steps*. In Easy Steps Limited, 2020.

جدول نموذج الأعمال BMC

<div></div> <div>الشركاء الرئيسيون (KP)</div> <div><ul style="list-style-type: none">شركة طباعة الهيكل الخارجيشركة صناعة اللوحات المطبوعةشركات التوصيل</div>	<div></div> <div>الأنشطة الرئيسية (KA)</div> <div><ul style="list-style-type: none">تصميم وصنع وتوريد المنتجخدمات ما بعد البيعتثبيت النظام للعملاءتطوير المنتج</div>	<div></div> <div>الموارد الرئيسية (KA)</div> <div><ul style="list-style-type: none">القطع الالكترونيةعامل في الجانب البرمجي والاخر في جانب الهيكل والتفكيتمويل ذاتي</div>	<div></div> <div>القيم المقترحة (VP)</div> <div><ul style="list-style-type: none">سعر مناسب مقارنة بالقيمة المقدمةمتكيف ومرن كل على حسب استخدامه ومقامهيحد من خطر ضياع المفاتيحيحد من خطر دخول الغرياءيحد من خطر ضياع الموارد الماديةنقصان العبء على الموظف وتوظيفه لاعمال اخرى</div>	<div></div> <div>العلاقة مع العملاء (CR)</div> <div><ul style="list-style-type: none">مساعد شخصيخدمة ذاتية من خلال كتيب للمنتجبرنامج يقوم باستخلاص المعلومات للعميل</div> <div></div> <div>قنوات توزيع (CH)</div> <div><ul style="list-style-type: none">وسائل التواصل الاجتماعي والبريد الالكترونياراء الزبائن في التجريبشراء وبيع عبر الانترنتالتوصيل عبر شركات التوصيلخدمات ما بعد البيع تصلح وتركيب وتثبيت للمنتج</div>	<div></div> <div>شرائح العملاء (CS)</div> <div><ul style="list-style-type: none">كلية العلوم والتكنولوجياجامعة غرداية ومن ثم كل الجامعة وكامل جامعات التراب الوطنياصحاب المؤسسات والشركاتذوي المناصب الحساسةاصحاب الفنادق وممتلكي المنازل</div>
<div></div> <div>هيكل التكاليف (CS)</div> <div><ul style="list-style-type: none">تكاليف الشركاءتكاليف شراء المنتجتكاليف المنصة الرقميةتكاليف العقاد حاسوب انترنت</div>	<div></div> <div>مصادر الدخل الإيرادات (RS)</div> <div><ul style="list-style-type: none">من خلال بيع المنتجمن خلال اشتراك سنوي في المنصةعن طريق اعلانات للمنصة المستعملة</div>				

• شرائح العملاء (Customer Segments - CS)

- كلية العلوم والتكنولوجيا – جامعة غرداية، ثم باقي الجامعة وكامل جامعات التراب الوطني: هذه الفئة تشمل المؤسسات الجامعية، بداية من كلية معينة كنقطة انطلاق (كلية العلوم والتكنولوجيا)، ثم التوسع لباقي كليات جامعة غرداية، ثم نحو كل جامعات الجزائر بحيث الجامعات تحتاج إلى أنظمة ذكية لمراقبة الدخول والخروج، أنظمة حضور للأساتذة والطلبة، أنظمة حماية للمخابر أو القاعات الحساسة، أو حتى أنظمة لمراقبة المعدات أو تأمين الوثائق.
- أصحاب المؤسسات والشركات: تشمل هذه الفئة مسؤولي ومديري المؤسسات بمختلف أنواعها (خاصة أو عمومية)، صغيرة أو كبيرة، سواء كانت صناعية، تجارية أو خدمية من أجل حماية ممتلكات الشركة، مراقبة الولوج لمناطق حساسة، تنظيم دخول الموظفين والزوار، أنظمة حضور وانصراف.
- ذوي المناصب الحساسة: تشمل هذه الفئة الأشخاص الذين يشغلون مناصب ذات طبيعة حساسة مثل مدراء تنفيذيين، مسؤولين أمنيين، باحثين، أو موظفين في قطاعات ذات طابع سري أو مهم من أجل حماية الوصول إلى المعلومات أو الأماكن، أنظمة تحقق قوية (بصمة، وجه، كود سري)، تسجيل كل محاولة دخول.
- أصحاب الفنادق وممتلكي المنازل: هذه الفئة تضم الأفراد أو المستثمرين الذين يملكون فنادق، شقق للإيجار أو منازل ذكية، ويرغبون في إدارة الدخول والتحكم عن بعد نظام دخول بدون مفاتيح، مراقبة عبر الإنترنت، تحكم في الإضاءة أو التدفئة، إشعارات فورية عند وجود حركة مشبوهة.

• العلاقة مع العملاء (Customer Relationship - CR)

- مساعد شخصي يجيب على الأسئلة: هذا يشير إلى وجود شخص يكون متاحًا للرد على استفسارات العملاء بشكل مباشر. أمثلة:
 - 1- الرد على أسئلة حول طريقة تركيب المنتج
 - 2- تقديم الدعم الفني في حالة وجود مشكلة.
 - 3- تقديم نصائح لاستخدام فعال للمنتج.
 - 4- الفائدة للعملاء: يشعر العميل بالثقة لأنه يتلقى مساعدة فورية وشخصية عند الحاجة.
 - 5- الفائدة للمشروع: بناء علاقة قوية مع العميل وتحسين رضاه وبالتالي تعزيز الولاء.
- خدمة ذاتية من خلال كتيب للمنتج: هذه وسيلة لتمكين العميل من حل مشاكله أو فهم كيفية استخدام المنتج دون الرجوع إلى الدعم المباشر، من خلال دليل شامل ومبسّط.

ما يحتويه الكتيب:

- خطوات تركيب أو تفعيل النظام.
- كيفية إضافة مستخدم جديد أو تغيير الإعدادات.
- حلول للمشاكل الشائعة.
- برنامج يقوم باستخلاص المعلومات للعميل: هذا يشير إلى أداة أو برنامج ذكي يقوم تلقائيًا بتحليل بيانات المستخدم أو استخدامه للمنتج ويقدم له تقارير أو معلومات مفيدة.

أمثلة:

- 1- عرض تقارير دخول وخروج المستخدمين في نظام التحكم.
- 2- إحصائيات حول من يستخدم النظام أكثر، وفي أي وقت.
- 3- تنبيهات في حال وجود أنشطة غير عادية.

• قنوات التوزيع (Channels - CH)

- وسائل التواصل الاجتماعي والبريد الإلكتروني: استخدام منصات مثل فيسبوك، إنستغرام، لينكدان، تويتر بالإضافة إلى البريد الإلكتروني كقنوات للتسويق والتواصل. الدور في القناة:
 - 1- جذب انتباه العملاء المحتملين.
 - 2- نشر معلومات حول المنتج أو العروض.
 - 3- التفاعل والرد على الاستفسارات.
- آراء الزبائن في التجريب: الاعتماد على تجربة الزبائن الأوائل ونقل آرائهم وتقييماتهم كوسيلة ترويج فعالة (تسويق شفهي أو ما يسمى بـ Word of Mouth) مثال إيميالات أو قوغل فورم.

كيف تعمل كفتاة؟:

- 1- عرض قصص النجاح أو تجارب إيجابية.
 - 2- تشجيع العملاء على التوصية بالمنتج لغيرهم.
 - 3- نشر مراجعات أو فيديوهات توضيحية من العملاء.
- شراء وبيع عبر الإنترنت: توفير إمكانية شراء المنتج عبر موقع إلكتروني، متجر إلكتروني، أو منصات البيع مثل جوميا أو أمازون.

ما تتضمنه القناة:

- 1- عرض مفصل للمنتج (صور، مواصفات، سعر).
 - 2- بوابة دفع إلكتروني (بطاقة بنكية، بريدي موب، CIB...).
 - 3- متابعة حالة الطلب من قبل الزبون.
- التوصيل عبر شركات التوصيل: التعاون مع شركات مختصة في التوصيل مثل EMS، Yalidine، Jumia Express، أو شركات محلية لنقل المنتج إلى الزبون.

دور القناة:

- 1- تسريع وصول المنتج.
 - 2- تقديم خيارات تتبع الطلب.
 - 3- إمكانية الدفع عند الاستلام. (COD)
- خدمات ما بعد البيع (تصليح، تركيب، تثبيت): تقديم دعم تقني بعد عملية البيع، يشمل:

- 1- إرسال فني لتركيب النظام أو المنتج.
 - 2- توفير الصيانة في حال وجود عطل.
 - 3- تقديم تحديثات أو تحسينات مستقبلية.
- القيم المقترحة (Value Proposition - VP) :

- يحصل العميل على حل ذكي ومحترف دون الحاجة لإنفاق مبالغ ضخمة.
- يشعر العميل أن النظام مصمم خصيصاً له، وليس حلاً عاماً فقط.
- لا خوف من ضياع المفاتيح، ولا حاجة لاستبدال الأقفال، مما يوفر وقتاً ومالاً.
- حماية أفراد المؤسسة أو الأسرة من التسلل أو الاعتداء.
- تقليل الخسائر المادية وزيادة الشعور بالأمان.
- تخفيض التكاليف، واستغلال الموظفين في مهام أخرى أكثر إنتاجية.
- يشعر العميل أنه مدعوم في كل وقت، سواء بوسائل بشرية أو تقنية.
- العميل لا يواجه تعقيدات في تشغيل النظام أو صيانته، مما يزيد من راحته وثقته.
- يمكن للعميل معرفة من دخل ومتى، واتخاذ قرارات بناءً على بيانات حقيقية.
- سعر أقل من المنتج المستورد.
- تشجيع العمالة المحلية.
- تجربة عميل متكاملة، من الطلب إلى التشغيل، دون عناء.

• مصادر الدخل (Revenue Streams - RS) :

- من خلال بيع المنتج: بيع النظام أو الجهاز (مثلاً: لوحة تحكم، وحدة فتح الباب، قارئ البصمة، إلخ) كمنتج مادي يُباع مرة واحدة.

شكل الدخل:

- 1- مبلغ ثابت مقابل كل جهاز أو حزمة.

2- يمكن تقديم خيارات متنوعة (نسخة أساسية، متقدمة، احترافية).

الفائدة:

- 1- تمويل مباشر وسريع عند كل عملية بيع.
- 2- يمنح العملاء حرية شراء الجهاز وتثبيته دون التزام طويل.

- من خلال اشتراك سنوي في المنصة: توفير منصة إلكترونية (Dashboard) أو تطبيق ويب (تُستخدم لإدارة النظام عن بُعد (إضافة مستخدمين، مراقبة الدخول، تصدير تقارير، تحديث البرمجيات...)).

شكل الدخل:

- 1- اشتراك سنوي (أو شهري) مقابل الوصول إلى المنصة.
- 2- يمكن تقديم باقات مختلفة حسب عدد الأبواب أو المستخدمين.

الفائدة:

- 3- دخل مستمر (Recurring Revenue).
 - 4- يشجع على ولاء العميل وبقائه ضمن نظامك.
- عن طريق الإعلانات على المنصة المستعملة: عرض إعلانات موجهة داخل المنصة أو التطبيق الذي يستخدمه العملاء. هذه الإعلانات قد تكون:

- 1- لأدوات أو خدمات مكملة (كاميرات، شركات صيانة، أجهزة استشعار...).
- 2- لشركاء أو معلنين مهتمين بشريحة عملائك.

شكل الدخل:

- 1- مقابل مادي لكل إعلان (CPC أو CPM).
- 2- دخل من شراكات تجارية.

الفائدة:

- 1- مصدر دخل إضافي دون تكلفة على العميل.
- 2- استغلال عدد المستخدمين النشطين في توليد ربح من الإعلانات

- اقتراحات لإضافة مصادر دخل مستقبلية:

- 1- خدمات ما بعد البيع مدفوعة: مثل تركيب، تدريب، أو صيانة خاصة.
- 2- بيع تراخيص للتركيب للشركات المحلية
- 3- تحصيل رسوم مقابل دعم فني متميز (Premium Support).
- 4- تخصيص النظام حسب الطلب (Customization).

• الأنشطة الرئيسية (Key Activities - KA):

- تصميم وصنع وتوريد المنتج:

- 1- تصميم الحل التقني من الناحية البرمجية (Software) والعتادية (Hardware).
- 2- تطوير الدارات الإلكترونية، الهيكل، والبرمجيات المدمجة.

- 3- الإشراف على صناعة المنتج أو تجميعه، سواء داخليًا أو بالتعاون مع مصنعين خارجيين.
- 4- تنظيم توريد المكونات (حساسات، وحدات بصمة، شاشات، متحكمات...).

- خدمات ما بعد البيع:

- 1- توفير الدعم الفني للعملاء بعد شراء المنتج.
 - 2- تقديم خدمات الصيانة، التحديثات، والإصلاح عند الحاجة.
 - 3- الرد على استفسارات العملاء، وضمان رضاهم.
- #### - تثبيت النظام للعملاء:
- 1- إرسال فريق تقني أو توفير كتيبات وإرشادات لتثبيت النظام في الجامعات، المؤسسات، أو المنازل.
 - 2- ضمان تشغيل النظام بسلاسة وربطه بالشبكة والمنصة الإلكترونية.

- تطوير المنتج:

- 1- تحسينات دورية على المنتج بناءً على ملاحظات العملاء أو تغيرات السوق.
- 2- إضافة خصائص جديدة (مثل دعم وجوه، التحكم من الهاتف، الذكاء الاصطناعي...).
- 3- تحديث البرمجيات والتقنيات المستخدمة لمواكبة التطور.

• الموارد الرئيسية (Key Ressources - KR) :

- القطع الإلكترونية:

- 1- تشمل جميع المكونات المادية اللازمة لتجميع النظام مثل:
 - المتحكمات الدقيقة (مثل ESP32 أو Arduino)
 - حساس البصمة
 - قفل كهربائي (Relay أو Solenoid Lock)
 - وحدات الاتصال (Wi-Fi, LoRa...)
 - مزودات الطاقة، الأسلاك، القطع المطبوعة (PCB)

2- أهمية المورد:

- هي المكونات الأساسية التي يقوم عليها الجهاز.
- تؤثر جودتها على أداء المنتج ورضا المستخدم

- عامل في الجانب البرمجي وآخر في الجانب الهيكلي والتقني:

المورد البشري هو من أهم عناصر نجاح المشروع، وينقسم إلى:

- 1- مبرمج/مطور برمجيات: مسؤول عن تطوير الأكواد، برمجة المتحكمات، تصميم واجهات الويب أو التطبيق.
- 2- تقني/مهندس إلكترونيات: يعتني بتصميم الدوائر، تجميع المكونات، اختبار الأجهزة، والإشراف على الجانب الميكانيكي أو الهيكلي (علبة الجهاز، التركيب الفيزيائي...).

- تمويل ذاتي:

- في المرحلة الأولى من المشروع، يتم تمويله من الموارد الشخصية للفريق المؤسس دون الحاجة إلى مستثمر خارجي.

- يغطي التمويل: شراء المكونات، الأدوات، تكاليف الاختبار، التصميم، وربما التسويق الأولي.

- تمويل عبر البنك:

- مع كبر المشروع نحتاج رأس مال أكبر وبالتالي نلجأ للبنك.

2- أهمية المورد:

- يمنح الاستقلالية في اتخاذ القرار.
- يُظهر الجدية والالتزام عند البحث لاحقًا عن مستثمرين أو دعم مالي خارجي.

• الشركاء الرئيسيون (Key Partners - KP) :

- شركة طباعة الهيكل الخارجي:

- 1- شركة متخصصة في تصميم وطباعة الهياكل الخارجية للمنتج (Case/Boitier) ، سواء باستخدام:
- 2- الطباعة ثلاثية الأبعاد (3D Printing) :
- 3- أو قولبة بلاستيكية/معدنية حسب الحاجة

4- يمكن تصميم الهيكل ليكون مقاومًا للعوامل الجوية (عند الحاجة)، سهل التركيب، ومناسبًا للأغراض الجمالية والأمنية.

- شركة صناعة اللوحات المطبوعة (PCB) :

- 1- شريك تقني مسؤول عن إنتاج اللوحات الإلكترونية المطبوعة (Printed Circuit Boards) الخاصة بالمشروع بناءً على التصميمات المقدمة.
- 2- يتكفل أيضًا بتركيب المكونات الإلكترونية (SMD/THT) في حالة الإنتاج بكميات كبيرة.
- شركات التوصيل:
- 1- شركات مختصة في شحن وتوصيل المنتج إلى الزبائن سواء داخل المدينة أو في مدن أخرى.
- 2- تشمل خدماتها التوصيل السريع، التتبع، وضمان وصول المنتج في حالة سليمة.

• هيكل التكاليف (Cost Structure - CS) :

- تكاليف الشركاء:
- 1- تمثل الأموال المدفوعة للشركاء الخارجيين مقابل الخدمات التي يقدمونها، مثل:
- 2- طباعة الهيكل الخارجي
- 3- تصنيع وتركيب اللوحات الإلكترونية (PCB)
- 4- خدمات التوصيل إلى الزبائن
- تكاليف شراء المنتج:
- 1- المتحكمات الدقيقة (مثل ESP32)
- 2- حساس البصمة أو الكاميرا
- 3- شاشة العرض
- 4- القفل الإلكتروني
- 5- كابلات، أسلاك، مقاومات، وحدات تغذية...
- تكاليف المنصة الرقمية:
- 1- استضافة الخادم (Hosting)
- 2- اسم النطاق (Domain)
- 3- صيانة وتحديث الموقع أو التطبيق
- 4- تأمين البيانات وحمايتها (Cybersecurity)
- تكاليف العتاد:
- 1- شراء أو صيانة الحواسيب المستخدمة في البرمجة والتصميم
- 2- اشتراك الإنترنت عالي السرعة
- 3- أدوات العمل المكتبي (طابعات، ماسحات، برمجيات التصميم)

• الاسم التجاري للمؤسسة SmartGate :

"SmartGate" هو اسم يجمع بين كلمتين:

- Smart = ذكي، يشير إلى استخدام تقنيات حديثة.
- Gate = بوابة، ترمز إلى أبواب المختبرات والمرافق الجامعية.

يعكس الاسم هدف المشروع في تقديم نظام دخول ذكي وآمن يعتمد على تقنيات مثل البصمة، الكاميرا، والرموز السرية.

الشعار (Slogan) :

"دخول آمن، ذكاء مستدام"

• العلامة التجارية:



SmartGate

"دخول آمن، ذكاء مستدام"



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة غرداية
حاضنة أعمال جامعة غرداية



رقم: 276 / ح.أ.ج.غ/2025

شهادة توظيف مشروع مبتكر وفق القرار 008 المعدل والمتمم للقرار 1275

أنا الممضي أسفله، السيد: د/ طالب أحمد نور الدين

مسير حاضنة الأعمال: جامعة غرداية

المقر الاجتماعي/ العنوان: المنطقة العلمية، ص ب 455، غرداية، 47000، الجزائر

بتاريخ: 2025/04/10

رقم علامة الحاضنة: 1004253146

طبيعة المشروع: مؤسسة ناشئة

أشهد أن الطالب(ة) / الطلبة التالية أسماؤهم:

الإسم واللقب	الطور الدراسي	التخصص	الكلية
محمد أبي اسماعيل	M2	آلية وأنظمة	العلوم والتكنولوجيا
عمر بورورو	M2	آلية وأنظمة	العلوم والتكنولوجيا

تحت إشراف الأستاذ(ة)/الأستاذة التالية أسماؤهم:

الإسم واللقب	الرتبة	التخصص	الكلية
شرف عبد الكريم مصباح	أستاذ محاضر ب	آلية	العلوم والتكنولوجيا
بكار بلقاسم	أستاذ محاضر أ	آلية	العلوم والتكنولوجيا

تم توظيفه على مستوى حاضنة أعمال جامعة غرداية - بمشروع تحت اسم:

Intelligent system for access control and management in the laboratories of the
faculty of science and technology.

خلال السنة الجامعية: 2025/2024

سلمت هذه الشهادة بطلب من المعني للإدلاء بها في حدود ما يسمح به القانون.

حرر في غرداية بتاريخ: 17/06/2025

مدير الحاضنة



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

Université de Ghardaïa

Faculté des Sciences

et de la technologie



جامعة غرداية

كلية العلوم والتكنولوجيا

قسم: الآلية والكهروميكانيك

غرداية في: 01 جويلية 2025

شعبة: الآلية

تخصص: آلية وأنظمة

شهادة ترخيص بالتصحيح والايذاء:

انا الاستاذ(ة): ربيعي عيسى

بصفتي المشرف المسؤول عن تصحيح مذكرة تخرج ماستر المعنونة بـ:

Intelligent System for Access Control and Management in the
Laboratories of the Faculty of Science and Technology

من انجاز الطالب (الطالبة):

ABISMAIL MOHAMMED

BOUROUROU OMAR

التي نوقشت بتاريخ: 25/06/2025

اشهد ان الطالب/الطالبة قد قام/قاموا بالتعديلات والتصحيحات المطلوبة من طرف لجنة المناقشة وقد تم التحقق من ذلك من طرفنا وقد استوفت جميع الشروط المطلوبة.



امضاء المسؤول عن التصحيح