



UMM AL-QURA UNIVERSITY
Computer Engineering Department

FaceID Lock

A project submitted
in partial fulfillment of the requirements for the degree of
Bachelor in the Department of Computer Engineering

by

Mohammed Al-Zahrani (439013299)

Saleh Al-Maliki (441001301)

Rafea Al-Amri (439010330)

Supervised by

Dr: Bander Alshaw

November / 2024

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to Dr. Bander Alshawi for his invaluable support and guidance throughout this project. Dr. Ammar's expertise, mentorship, and unwavering commitment to academic excellence have been instrumental in successfully completing this project.

His insightful feedback, encouragement, and willingness to share knowledge have significantly contributed to our growth as students and the overall quality of this project. We sincerely appreciate his dedication to our academic and personal development.

Dr. Bander Alshawi contributions have not only enriched this project but have also been a source of inspiration for future endeavors. We are truly thankful for his guidance and support.

UNDERTAKING

This section is to declare that the project entitled " FaceID Lock" is an original work done by the undersigned, in partial fulfillment of the requirements for the degree "Bachelor in the Department of Computer Engineering" at Computer Engineering Department, College of computers and information systems, Umm Al-Qura University.

All the analysis, design, and system development have been accomplished by the undersigned. Moreover, this project has not been submitted to any other college or university.

Student 1: Mohammed Al-Zahrani

Email Address: s439013299@st.uqu.edu.sa

Student 2: Saleh Al-Maliki

Email Address: s@st.uqu.edu.sa

Student 3: Rafea Al-Amri

Email Address: s439010330@st.uqu.edu.sa

Note: sign across your name

ABSTRACT

Efficient and secure access control systems are crucial for modern facilities, where traditional key-based or card-based systems present vulnerabilities and management challenges. Manual access control methods are susceptible to key duplication, card theft, and unauthorized sharing, leading to security risks and resource management issues. Therefore, there is a pressing need for a biometric-based solution that combines facial recognition with electronic door control systems.

The target problem is to develop an advanced FaceID Lock system that integrates facial recognition technology with electronic door locks, providing seamless and secure access control. This system aims to accurately identify authorized individuals and automatically control door access while maintaining a comprehensive log of entry and exit activities.

The proposed method leverages convolutional neural networks (CNNs) for facial recognition, coupled with smart electronic lock mechanisms. This integrated approach provides a robust and secure access control solution. The system's key components include CNN-based facial feature extraction, a secure database of authorized users, electronic lock control mechanisms, and real-time access monitoring capabilities.

The system undergoes testing using diverse facial datasets and various environmental conditions to ensure reliable operation. This evaluation helps assess both the accuracy of facial recognition and the responsiveness of the electronic lock mechanism in real-world scenarios.

The expected results include automated door access control, real-time unauthorized access prevention, secure entry/exit logging, and a centralized management interface. The system also features immediate lock activation/deactivation based on facial recognition results and maintains detailed access records.

The achieved results demonstrate a significant advancement in access control technology, combining the security of biometric authentication with the convenience of automated door control. This innovative system offers a more secure, efficient, and user-friendly solution compared to traditional access control methods, while providing comprehensive monitoring and management capabilities.

Table of Contents

ACKNOWLEDGEMENT.....	2
UNDERTAKING	3
ABSTRACT.....	4
Table of Contents.....	5
1. Problem Statement.....	11
1.1 Needs Identification.....	11
1.1.1 Raw Data (information)	11
1.1.2 Marketing Requirements.....	12
1.1.3 Objective Tree.....	14
1.1.4 Ranking of Objective Tree.....	15
1.1.5 Ranked Objective Tree.....	21
1.2 Research Survey or Literature Review or Related Work or State-of-the-art	22
1.2.1 Background	22
1.2.2 Research Survey.....	22
1.2.3 Related Work	24
1.3 Need and Objective Statements.....	27
1.3.1 Need Statement.....	27
1.3.2 Objective Statement.....	28
2.....Requirements Specifications	29
2.1 Engineering Requirements	29
2.2 Constraints.....	31
2.2.1 Functionality	31
2.2.2 Performance	31
2.2.3 Manufacturability	31
2.2.4 Economic.....	31
2.2.5 Reliability and Availability.....	31
2.3 Standards.....	32
2.3.1 Testing.....	32
2.3.2 Safety	32

2.3.3	Design	32
3.	Design Space Exploration OR Concepts Generation and Evaluation.....	33
3.1	Concepts Generation	33
3.1.1	Concept Generation Table for System:	33
3.1.2	Concept Generation Table for Cameras	34
3.1.3	Concept Generation Table for Interaction	35
3.2	Concepts Evaluation	37
3.2.1	AHP Table for System:	37
3.2.2	Types of Cameras AHP	38
3.2.3	AHP Table for Interaction	38
4. Project Timeline Gannet Chart System Structure	40
4.1	Design Process Timeline and Chart:	40
4.2	System Design Timeline and Chart:	41
4.3	System Implementation Timeline and Chart:	42
4.4	System Testing Timeline and Chart:	43
4.5	Full Project Timeline and Chart:	44
5.	System Technical Approach	46
5.1	System Hardware Components	46
5.1.1	Orangepi	46
5.1.2	Using USB web cam	46
5.1.3	12VDC Solenoid Door Lock	47
5.1.4	Noise sensor.....	47
5.1.5	Magnetic Door Sensor	47
5.1.6	PIR Sensor	48
5.1.7	Open Door from Mobile	49
5.1.8	Save Opened Door Record (Date-Time)	49
5.2	System Software	50
5.2.1	OpenCV Library	50
5.2.2	Trained Model (Face Recognition).....	50
5.2.3	Python.....	50
5.3	System Flow Chart	51
5.3.1	New User Facial Features Extraction Flow Chart.....	51

5.3.2	System Process Flow Chart	52
5.3.3	Tracking Flow Chart	53
6.	References	59

LIST OF FIGURES

Figure 1: Non–Ranked Objective Tree	14
Figure 2: Ranked of Face ID Lock System	16
Figure 3: Ranked of Availability	17
Figure 4: Ranked of Security Features	17
Figure 5: Ranked of Quality	18
Figure 6: Ranked of Cost Effectiveness	19
Figure 7: Ranked of Maintenance	20
Figure 8: Ranked of User-Friendly Operation.....	21
Figure 9: Ranked Objective Tree	21
Figure 10: Facial Recognition using Convolutional Neural Networks	23
Figure 11: 3D Face Modeling	23
Figure 12: Vision Pass by Idemia	25
Figure 13: MeraFace by Videonetics.....	26
Figure 14: MinMoe by Hikvision.....	26
Figure 15: Comparison of state-of-the-art methods	27
Figure 16: IEC Logo[8]	32
Figure 17: SASO Logo [10]	32
Figure 18: System Design Timeline Chart.....	41
Figure 19: System Design Timeline Chart.....	42
Figure 20: System Implementation Timeline Chart	43
Figure 21: System Testing Timeline Chart.....	44
Figure 22: Full Project Timeline Chart	45
Figure 23: orangePi.....	46
Figure 24: USB web cam	46
Figure 25: 12VDC Solenoid Door Lock	47
Figure 26: noise sensor	47
Figure 27: magnetic door sensor	48
Figure 28 PIR Sensor.....	48
Figure 29: New User Facial Features Extraction Flow Chart	51

Figure 30: System Process Flow Chart	52
Figure 31: Tracking Flow Chart	53

LIST OF TABLES

Table 1: Face ID Lock System AHP	15
Table 2: Availability AHP	16
Table 3: Security Features AHP	17
Table 4: Quality AHP	18
Table 5: Cost Effectiveness AHP	18
Table 6: Maintenance AHP	19
Table 7: User-Friendly Operation AHP	20
Table 8: Engineering Requirements.....	30
Table 9: Concept Generation Table for System.....	33
Table 10: Concept Generation Table for Cameras.....	34
Table 11: Concept Generation Table for Interaction	36
Table 12:AHP for System.....	37
Table 13: AHP for Cameras.....	38
Table 14: AHP for Interaction	38
Table 15: Design Process Timeline	40
Table 16: System Design Timeline.....	41
Table 17: System Implementation Timeline	42
Table 18: System Testing Timeline	43
Table 19: Full Project Timeline	44

1. Problem Statement

Access control and security management remain critical challenges in various settings, from residential buildings to corporate environments. Traditional access control methods such as physical keys, access cards, or numeric keypads present significant security vulnerabilities and management complexities. There is an increasing need for more sophisticated, reliable, and user-friendly access control solutions that can effectively secure premises while providing convenient access to authorized individuals.

1.1 Needs Identification

The need analysis for the FaceID Lock system is conducted through systematic research and data collection, focusing on current market demands and technological capabilities.

1.1.1 Raw Data (information)

In today's digital era, facial recognition technology has become increasingly prevalent in security systems. The FaceID Lock system aims to enhance security measures by integrating facial recognition with electronic door locks. This system addresses several key challenges in current access control methods:

- **From a security perspective:**
Recognizing the need for advanced and efficient security, we focused on developing a solution for secure access control that minimizes human involvement. Through studies conducted in the Kingdom of Saudi Arabia, we examined the current security approaches used by companies to monitor access to sensitive areas, track personnel movements, and maintain a record of entry and exit activities.
- **Interviews with security experts:**
Through interviews with security professionals, we found that many companies require a combination of traditional access control measures and large security teams to monitor each entry point adequately. Furthermore, it became clear that existing methods, like keycards and PIN codes, are vulnerable to misuse and can complicate secure access management.
- **Proposal during discussions:**
During meetings with potential stakeholders, we proposed the development of an integrated access control system combining facial recognition technology with an electronic lock mechanism. By employing convolutional neural networks (CNNs) for facial recognition, the system identifies authorized individuals and automatically controls the lock, enabling secure, hands-free access. Additionally, the system includes an audio sensor to capture surrounding sounds, which can further enhance security by recording potential incidents or unauthorized activities.

- **Reception from technical authorities:**

Technical stakeholders in several Saudi Arabian companies responded positively to the proposed system, recognizing the value of enhanced security, reduced reliance on physical security staff, and a more efficient access management process. The system's real-time notifications and accurate access tracking were seen as beneficial features, with the added advantage of cost savings by reducing the need for extensive security personnel.

1.1.2 Marketing Requirements

The marketing requirements, based on the raw data, are as follows: (Marketing requirements should be numbered and must be easy-to-understand sentences.

i. Enhanced Security

The proposed system integrates facial recognition technology with an electronic lock to provide a high level of security, ensuring that only authorized individuals can access the secured area based on biometric identification.

ii. Hands-Free Access Control

By utilizing facial recognition, the system allows for seamless, hands-free entry, eliminating the need for physical keys or access cards, which can be lost, stolen, or duplicated.

iii. Audio Monitoring

The inclusion of an audio sensor enables the system to record ambient sounds, adding an extra layer of security by monitoring for unusual activities or sounds, and providing valuable evidence if needed.

iv. Mobile Application Control

The system includes a user-friendly mobile application that allows for remote control of the electronic lock, enabling users to lock or unlock doors remotely, manage access permissions, and receive real-time notifications.

v. Comprehensive Access Logs

The system maintains detailed logs of all entry and exit activities, including timestamps, facial recognition data, and audio recordings when necessary, aiding in monitoring and auditing access.

vi. Automated Operation

The system operates autonomously, reducing the need for human intervention in the access control process by automatically recognizing authorized faces and controlling the lock mechanism accordingly.

vii. Real-Time Alerts

In the event of unauthorized access attempts or security breaches, the system sends real-time alerts to designated personnel via the mobile application, ensuring prompt response to potential threats.

viii. High Accuracy and Speed

Utilizing advanced convolutional neural networks (CNNs), the facial recognition component provides high accuracy and rapid identification, allowing authorized users quick access while preventing unauthorized entry.

ix. Easy Installation and Integration

The system is designed for easy installation and can be integrated with existing door hardware and security systems, minimizing setup time and costs.

x. Scalability

The system is scalable to accommodate multiple access points and a large number of users, making it suitable for residential, commercial, and institutional applications.

xi. Data Security

All collected data, including facial recognition data and audio recordings, are securely stored with encryption and strict access controls to protect user privacy and comply with data protection regulations.

xii. User-Friendly Interface

The mobile application and system interfaces are designed to be intuitive and easy to use, allowing users to navigate features and manage settings without technical expertise.

xiii. Customizable Settings

Administrators can customize various system settings such as access schedules, user permissions, alert preferences, and audio recording options to meet specific security requirements.

xiv. Continuous Operation

The system is designed for continuous operation, ensuring that access control and security monitoring are maintained at all times without interruption.

xv. Cost-Effective Solution

By reducing reliance on physical keys, access cards, and security personnel, the system offers a cost-effective solution for modern access control needs.

xvi. Quality and Reliability

Built with high-quality components and leveraging proven technologies, the system ensures reliable performance and long-term durability.

1.1.3 Objective Tree

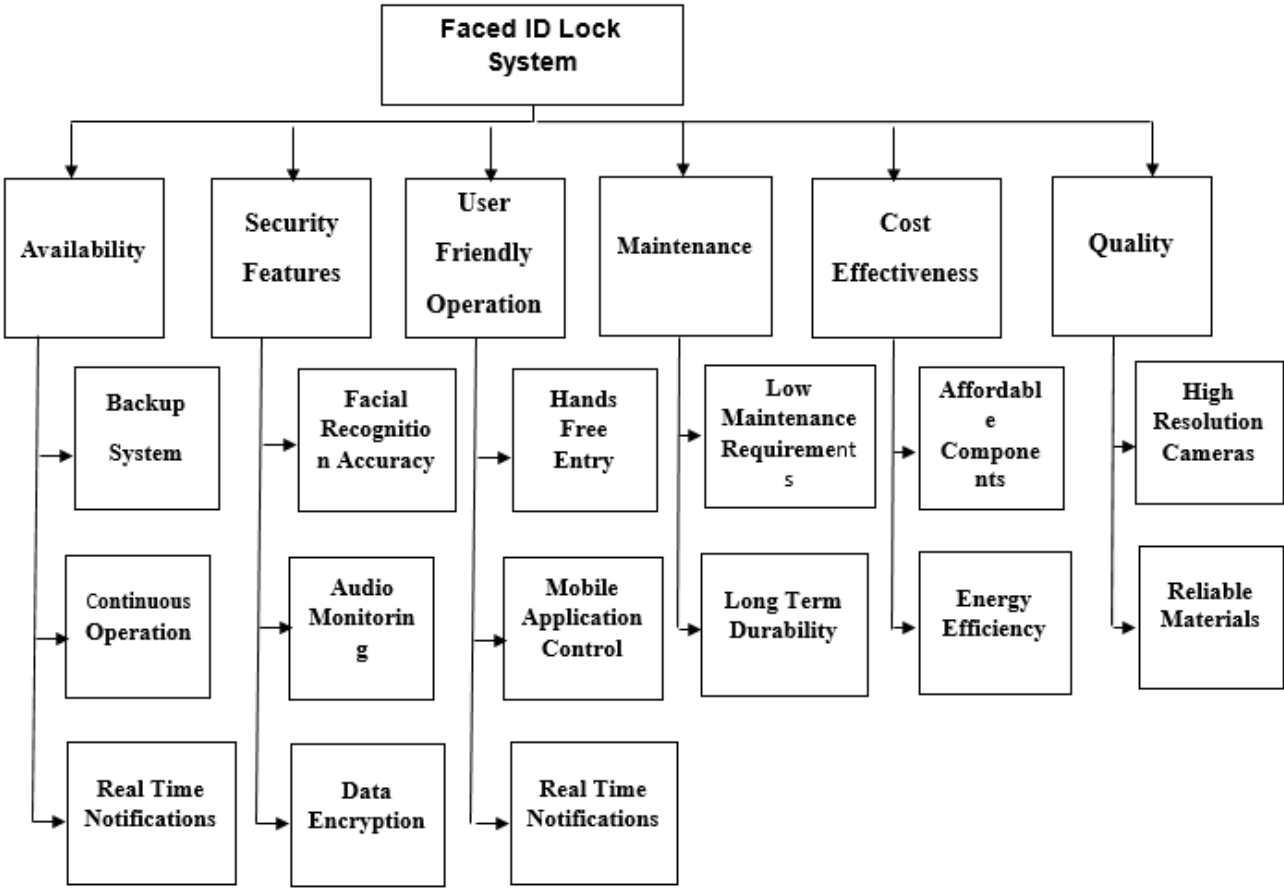


Figure 1: Non-Ranked Objective Tree

1.1.4 Ranking of Objective Tree

1.1.4.1 Face ID Lock System AHP

Table 1: Face ID Lock System AHP

Criterion	Availability	Maintenance	Cost Effectiveness	User-Friendly Operation	Security Features	Quality	GM	Weight
Availability	1	3	5	7	9	4	3.71	0.34
Maintenance	1/3	1	3	5	7	3	1.62	0.15
Cost Effectiveness	1/5	1/3	1	3	5	2	0.97	0.09
User-Friendly Operation	1/7	1/5	1/3	1	3	2	0.61	0.06
Security Features	1/9	1/7	1/5	1/3	1	3	0.56	0.05
Quality	1/4	1/3	1/2	1	3	1	1.04	0.09

This matrix for evaluating the *FaceID Lock System* is based on various criteria, including **Availability**, **Maintenance**, **Cost Effectiveness**, **User-Friendly Operation**, **Security Features**, and **Quality**. The numbers in the matrix reflect the relative importance or preference ratings for each criterion, with **Availability** considered the most critical component, given a weight of 0.34. This high weighting for **Availability** emphasizes the necessity for continuous, reliable operation in an access control system.

The matrix serves as an essential tool in decision-making, allowing stakeholders to quantify the significance of each criterion in assessing the *FaceID Lock System*. By providing a structured approach to evaluate the system's performance across multiple dimensions, stakeholders can ensure that the system meets the required standards in terms of reliability, ease of maintenance, affordability, user experience, security, and quality, with **Availability** receiving the highest priority in the evaluation process.

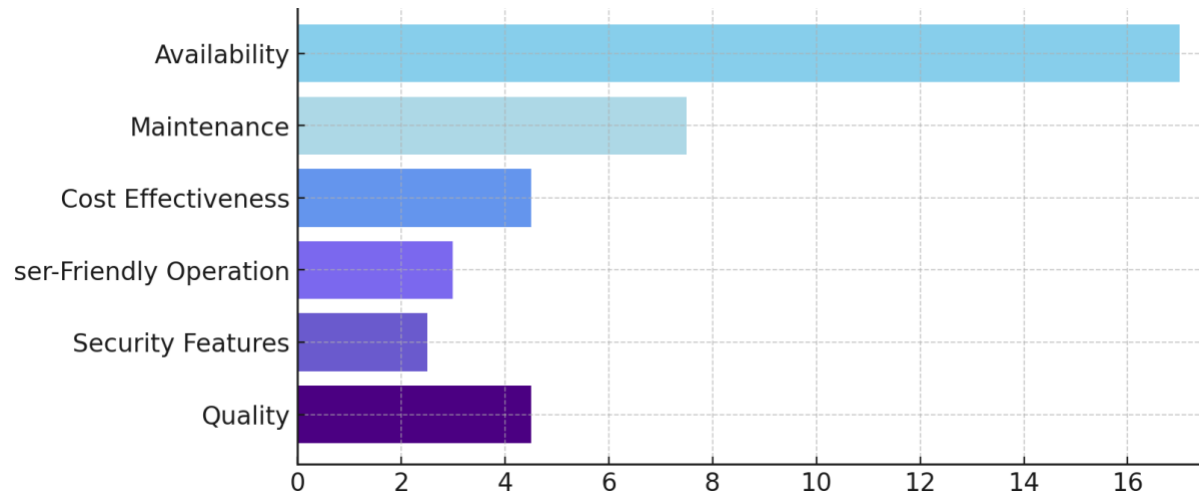


Figure 2: Ranked of Face ID Lock System

1.1.4.2 Availability AHP

Table 2: Availability AHP

Availability	Backup System	Continuous Operation	Real-Time Notifications	GM	Weight
Backup System	1	3	5	1.71	0.50
Continuous Operation	1/3	1	3	0.76	0.22
Real-Time Notifications	1/5	1/3	1	0.41	0.12

This matrix focuses on "Availability," evaluating three sub-criteria: "Backup System," "Continuous Operation," and "Real-Time Notifications." Among these, the **Backup System** is identified as the most critical sub-criterion, with a priority weight of 0.50, followed by **Continuous Operation** with a weight of 0.22, and **Real-Time Notifications** with a weight of 0.12. These priorities indicate each sub-criterion's importance in ensuring system availability, emphasizing the need for backup measures as the highest priority. This matrix serves as a valuable tool in decision-making by quantifying the significance of each sub-criterion, with **Backup System** having the highest weight in the availability assessment.

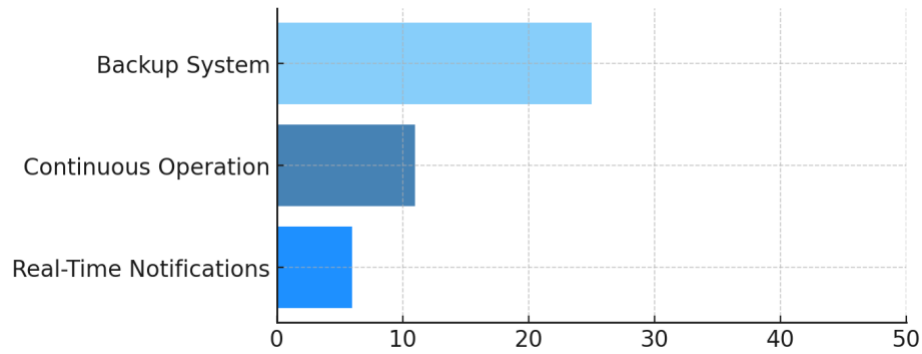


Figure 3: Ranked of Availability

1.1.4.3 Security Features AHP

Table 3: Security Features AHP

Security Features	Facial Recognition Accuracy	Audio Monitoring	Data Encryption	GM	Weight
Facial Recognition Accuracy	1	5	7	2.76	0.60
Audio Monitoring	1/5	1	3	0.76	0.20
Data Encryption	1/7	1/3	1	0.41	0.15

This matrix focuses on **Security Features**, evaluating three sub-criteria: **Facial Recognition Accuracy**, **Audio Monitoring**, and **Data Encryption**. Among these, **Facial Recognition Accuracy** is identified as the most critical sub-criterion, with a priority weight of 0.60, followed by **Audio Monitoring** with a weight of 0.20, and **Data Encryption** with a weight of 0.15. These priorities highlight each sub-criterion's importance in enhancing the system's security, with **Facial Recognition Accuracy** emphasized as the highest priority for preventing unauthorized access. This matrix serves as a valuable tool in decision-making, helping to quantify the significance of each sub-criterion, with **Facial Recognition Accuracy** holding the highest weight in the security assessment.

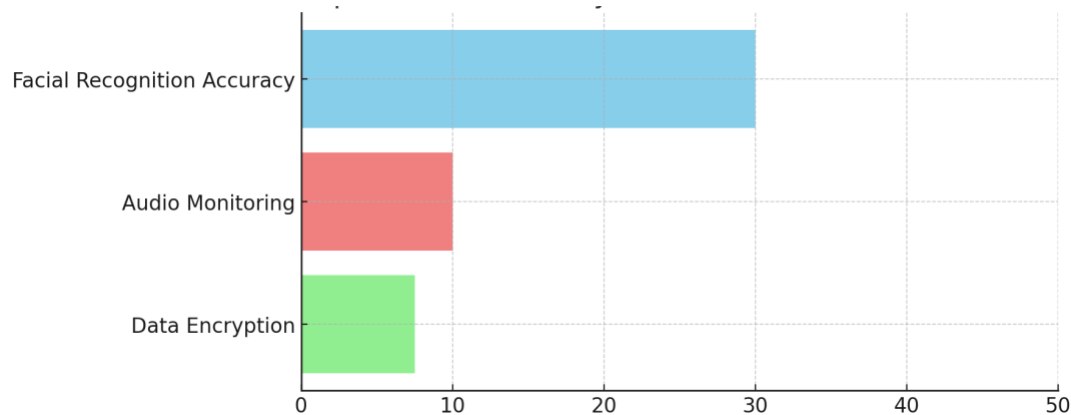


Figure 4: Ranked of Security Features

1.1.4.4 Quality AHP

Table 4: Quality AHP

Quality	High-Resolution Cameras	Reliable Materials	GM	Weight
High-Resolution Cameras	1	5	2.24	0.68
Reliable Materials	1/5	1	0.45	0.30

The **High-Resolution Cameras** criterion is prioritized with a weight of 0.68, underscoring the importance of image clarity and accuracy for effective facial recognition. **Reliable Materials** support long-term durability and resilience, with a weight of 0.30.

This AHP matrix aids decision-making by quantifying the importance of each quality-related sub-criterion, with **High-Resolution Cameras** having the highest impact on maintaining the FaceID Lock *System's* effectiveness.

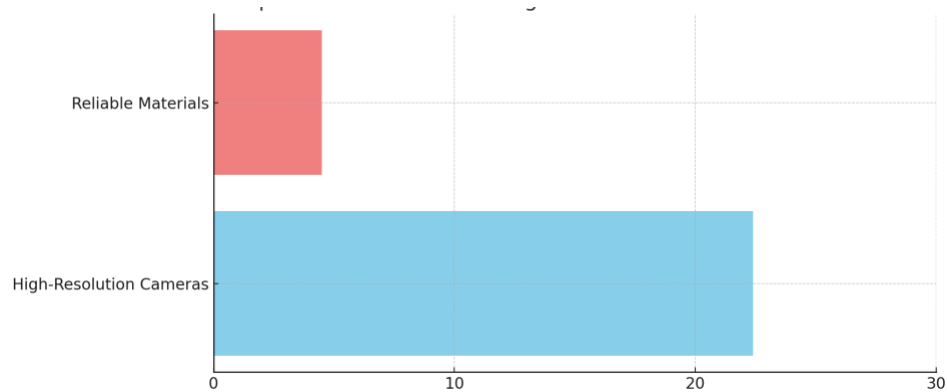


Figure 5: Ranked of Quality

1.1.4.5 Cost Effectiveness AHP

Table 5: Cost Effectiveness AHP

Cost Effectiveness	Affordable Components	Energy Efficiency	GM	Weight
Affordable Components	1	5	2.24	0.68
Energy Efficiency	1/5	1	0.45	0.30

The **Affordable Components** criterion holds the highest priority within **Cost Effectiveness**, with a weight of 0.68, underscoring its importance in minimizing the system's upfront costs.

Energy Efficiency, with a weight of 0.30, plays a supporting role by reducing ongoing energy expenses.

This AHP matrix helps in decision-making by quantifying the importance of each cost-related sub-criterion, with **Affordable Components** being the primary focus for ensuring the FaceID Lock *System* is economically viable.

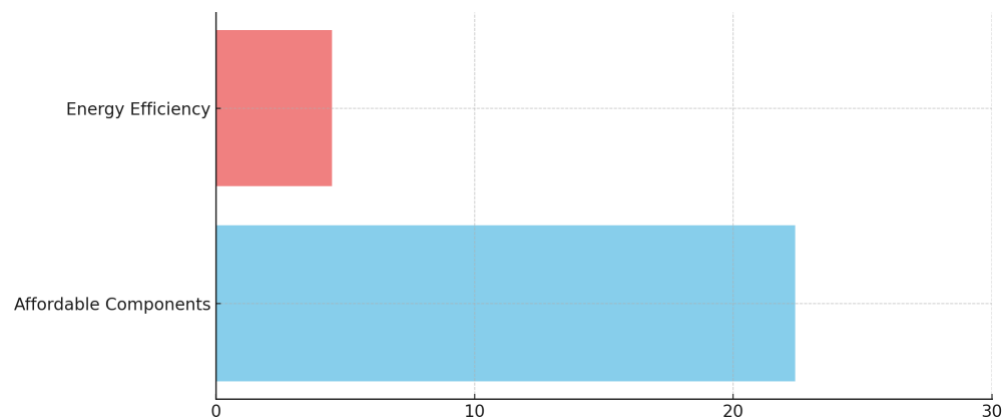


Figure 6: Ranked of Cost Effectiveness

1.1.4.6 Maintenance AHP

Table 6: Maintenance AHP

Maintenance	Low Maintenance Requirements	Long-Term Durability	GM	Weight
Low Maintenance Requirements	1	3	1.31	0.66
Long-Term Durability	1/3	1	0.51	0.33

The **Low Maintenance Requirements** criterion holds the highest priority within **Maintenance**, with a weight of 0.66, emphasizing the importance of reducing maintenance needs to ensure consistent system performance. **Long-Term Durability** is also significant but ranks lower, with a weight of 0.33, focusing on extending the system’s lifespan.

This AHP matrix aids in decision-making by quantifying the importance of each maintenance-related sub-criterion, with **Low Maintenance Requirements** being the primary focus in the maintenance assessment.

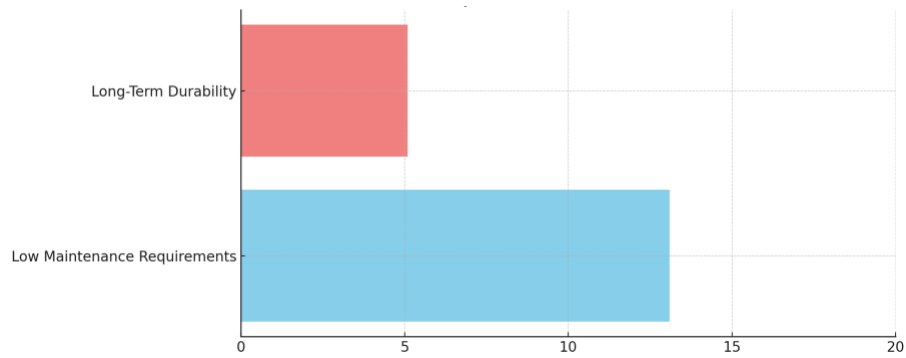


Figure 7: Ranked of Maintenance

1.1.4.7 User-Friendly Operation AHP

Table 7: User-Friendly Operation AHP

User-Friendly Operation	Hands-Free Entry	Mobile Application Control	Real-Time Notifications	GM	Weight
Hands-Free Entry	1	3	5	1.76	0.55
Mobile Application Control	1/3	1	3	0.76	0.23
Real-Time Notifications	1/5	1/3	1	0.41	0.15

The **Hands-Free Entry** criterion holds the highest priority within **User-Friendly Operation**, with a weight of 0.55, emphasizing the need for a touchless and convenient access experience. **Mobile Application Control** and **Real-Time Notifications** are also important, with weights of 0.23 and 0.15, respectively, as they contribute to the ease of operation and timely information for users.

This AHP matrix provides insight into the relative importance of each sub-criterion within **User-Friendly Operation**, with **Hands-Free Entry** as the primary focus to ensure an accessible and efficient user experience.

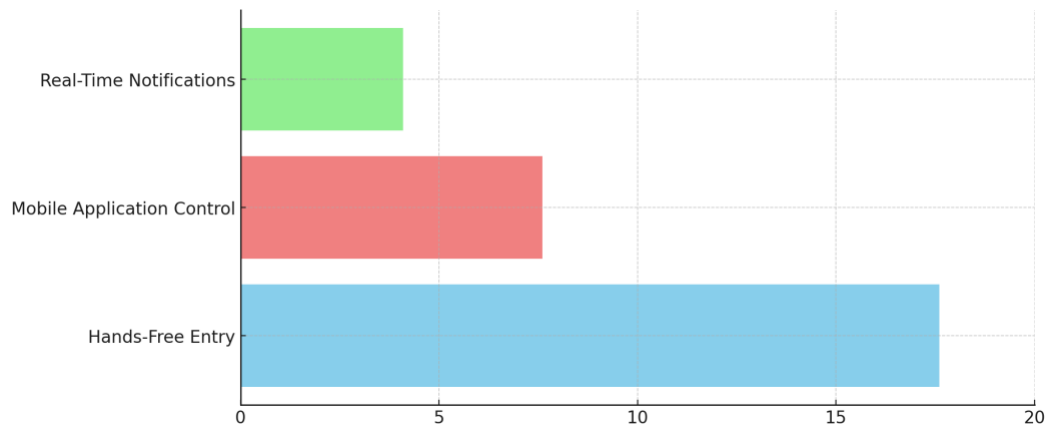


Figure 8: Ranked of User-Friendly Operation

1.1.5 Ranked Objective Tree

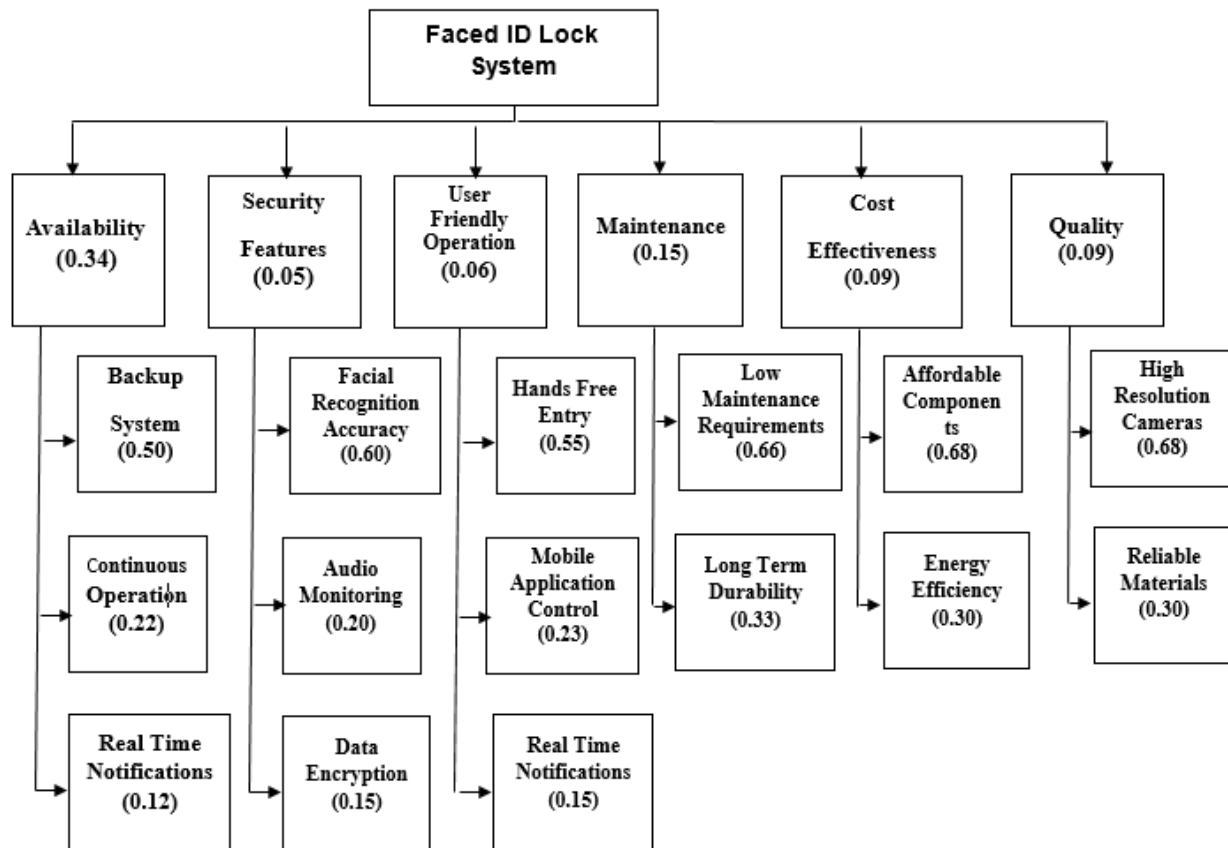


Figure 9: Ranked Objective Tree

1.2 Research Survey or Literature Review or Related Work or State-of-the-art

1.2.1 Background

Facial recognition technology has emerged as a significant tool in enhancing security and access control systems. By leveraging advancements in artificial intelligence (AI) and machine learning, facial recognition systems can identify and authenticate individuals based on their facial features, making it an effective solution for modern security needs. The FaceID Lock System utilizes AI-based facial recognition combined with additional security features, including audio monitoring and mobile application control, to offer a secure and user-friendly access control solution. This approach provides a seamless, contactless experience that is both efficient and highly reliable.

1.2.2 Research Survey

1. Facial Recognition using Convolutional Neural Networks (CNNs):

- CNNs have proven highly effective for facial recognition tasks due to their ability to capture spatial hierarchies in images. Research shows that CNN models, such as VGG-16 and ResNet-50, can achieve high accuracy in identifying faces when trained on large and diverse datasets. These architectures are widely used in facial recognition due to their capacity to handle complex patterns and variations in facial features. [1]
- Studies also demonstrate that combining CNNs with Support Vector Machines (SVM) for classification can enhance accuracy, especially in controlled environments. Pre-trained models, such as AlexNet and ResNet-50, are often employed for feature extraction, allowing systems to leverage existing knowledge and improve performance with less training data. [2]

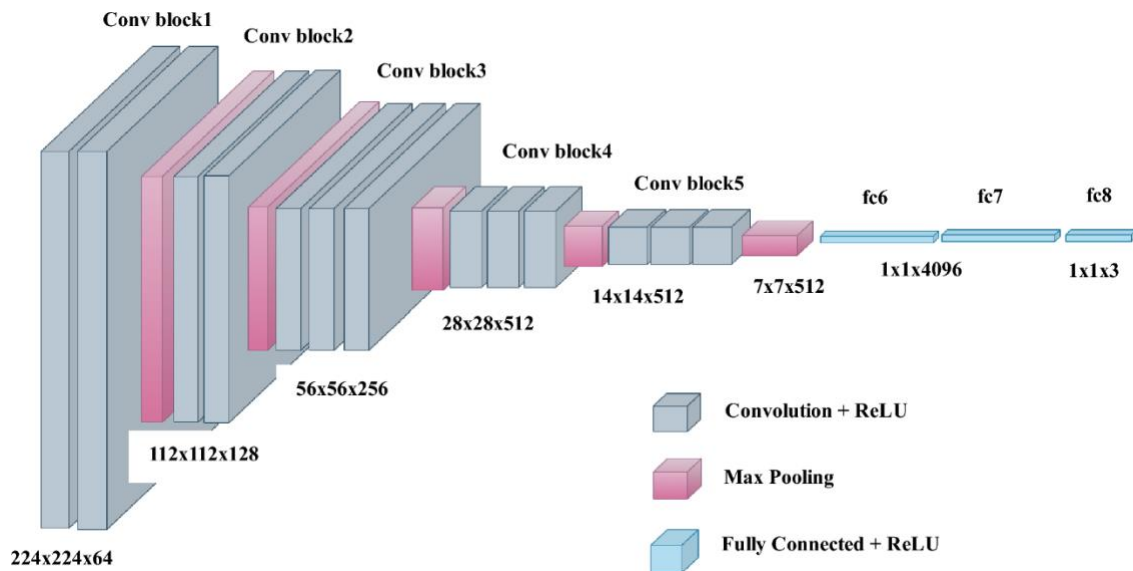


Figure 10: Facial Recognition using Convolutional Neural Networks

2. Challenges in Facial Recognition Accuracy:

- Research highlights that facial recognition systems can be affected by variations in lighting, facial expressions, and occlusions, such as glasses or masks. Techniques like 3D face modeling and the use of additional sensors have been explored to address these challenges. By mitigating these issues, systems can ensure more consistent accuracy in diverse conditions, which is critical for real-world applications like the *FaceID Lock System*. [3]

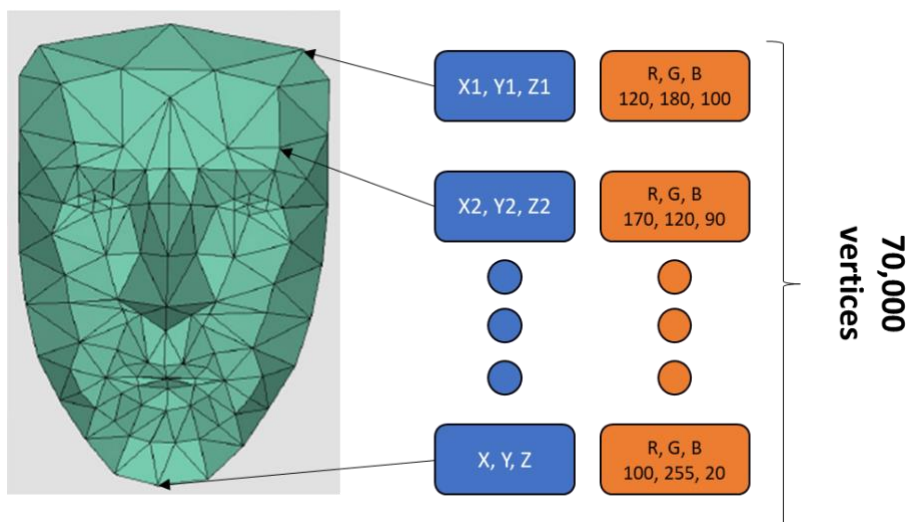


Figure 11: 3D Face Modeling

3. Mobile and IoT Integration for Enhanced User Experience:

- Integrating mobile applications and IoT technology into facial recognition systems enables users to remotely control and monitor access points. Studies indicate that this added convenience significantly improves user satisfaction and system flexibility. However, this integration also brings new security challenges, emphasizing the need for strong data encryption and secure communication protocols to prevent unauthorized access.[4]

1.2.3 Related Work

The following section reviews notable advancements and commercially available systems in facial recognition and access control, particularly focusing on systems that combine facial recognition with audio monitoring, energy efficiency, and mobile integration. These systems provide valuable insights and highlight the features that align closely with the objectives of the FaceID Lock System.

1. Vision Pass by Idemia

The work by Idemia, a pioneer in identity and security solutions, introduces the **Vision Pass** system, a cutting-edge facial recognition solution that redefines identity verification and access control. This system utilizes advanced 2D/3D imaging technology to achieve high accuracy by comparing facial features against a comprehensive company database. Vision Pass is known for its seamless user experience, swiftly verifying identities through rapid facial scans, eliminating the need for physical access cards or passwords.[5]

1. **Features:** Vision Pass supports a recognition range of up to one meter and operates effectively even when users wear masks. It is designed for both indoor and outdoor settings, featuring IP65 water resistance and IK07 impact resistance for durability. Additionally, Vision Pass provides anti-spoofing capabilities and supports multiple authentication methods, including facial recognition, access cards, mobile devices, and QR codes.
2. **Relevance:** This system's high accuracy and durability make it an exemplary model for secure access control, aligning with the goals of the *FaceID Lock System* to provide secure and user-friendly operation in various environments.



Figure 12: Vision Pass by Idemia

2. MeraFace by Videonetics

MeraFace by Videonetics is an advanced AI-driven facial recognition system that supports a wide array of applications, including identity management, law enforcement, surveillance, and access control. MeraFace utilizes a modular architecture, allowing it to operate across both on-premises and cloud environments, which offers flexibility for deployment.[6]

- **Features:** MeraFace supports distributed processing across multiple computing nodes, allowing video capture and facial identification functions to operate in multiple locations. Key features include anti-spoofing capabilities, high-speed recognition with response times of under 10 seconds for large databases, and compatibility with existing surveillance and video management systems.
- **Relevance:** The flexibility, modularity, and integration with various IP devices in MeraFace make it a relevant reference for the *FaceID Lock System*, which aims to support secure and scalable deployment options in diverse environments.

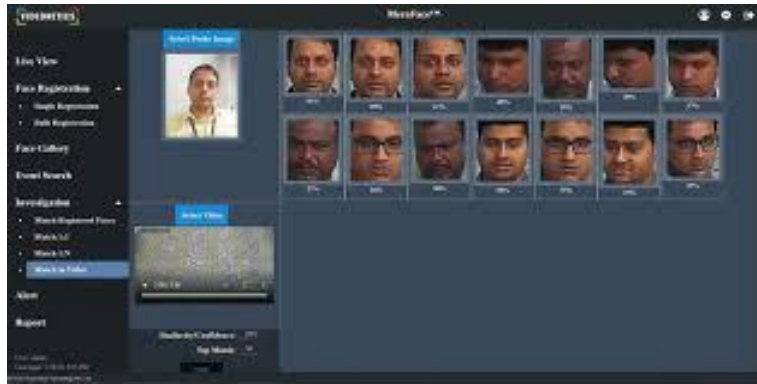


Figure 13: MeraFace by Videonetics

3. MinMoe by Hikvision

Hikvision's **MinMoe** terminals offer a touch-free experience for access control and attendance recording, prioritizing security, efficiency, and ease of use. MinMoe's facial recognition technology is known for its high accuracy and rapid verification, suitable for business environments where fast and reliable access is essential.[7]

- **Features:** MinMoe provides superior recognition speed (0.2 seconds) with a high accuracy rate (over 99%), alongside robust anti-spoofing technology and data encryption for secure access control. The system is adaptable with cloud-based and on-premises deployment options, making it a versatile choice for different business needs.
- **Relevance:** MinMoe's high-speed facial recognition, anti-spoofing technology, and adaptability to various environments make it an important reference for designing the *FaceID Lock System*, which seeks to deliver a secure and responsive access control experience.



Figure 14: MinMoe by Hikvision

1.2.3.1 Comparison of state-of-the-art methods

No	References	Availability	Maintenance	Cost Effectiveness	User-Friendly Operation	Security Features	Quality
1	[5]	Medium	High	Low	Low	High	High
2	[6]	Medium	Medium	Low	Medium	High	High
3	[7]	Medium	High	Low	Low	High	High

Figure 15: Comparison of state-of-the-art methods

Many companies offer solutions for facial recognition-based access control; however, most require compromises on certain features. For the **Availability** requirement, the systems on the market face limitations regarding the number of user profiles they can manage efficiently. In terms of the **AI Smart System** requirement, all three systems reviewed perform exceptionally well in accurate facial recognition and quick response times. For **Maintenance**, the systems in references [5] and [7] have an advantage as they offer local support, while the system in reference [6] lacks a regional branch, which may delay maintenance services in case of technical issues. Regarding the **User-Friendly Operation** requirement, only the system in reference [6] includes features that allow administrators to track user activity, adding an extra layer of management convenience. All three systems score low on the **Cost Effectiveness** requirement, as these advanced security solutions are generally high-cost investments. Lastly, when it comes to **Quality**, each system delivers a high standard, ensuring reliable performance and robust security features.

1.3 Need and Objective Statements

Based on insights gathered from customer requirements in Section 1.1 and the research survey conducted in Section 1.2, this section outlines the need statement (Section 1.3.1) and the objective statement (Section 1.3.2). These statements summarize the critical requirements and goals for the FaceID Lock System, reflecting the challenges and opportunities identified in the field of facial recognition access control.

1.3.1 Need Statement

The growing demand for secure, contactless access control solutions has led to a surge in facial recognition technologies. While several systems currently exist, they often involve trade-offs, such as high implementation costs, limited tracking capabilities, or restricted functionality in low-light conditions. The *FaceID Lock System* seeks to address these gaps by providing an efficient, accurate, and versatile solution that combines facial recognition with additional

features like audio monitoring and mobile app integration. This system is designed to offer a user-friendly experience while ensuring high security, reliability, and ease of maintenance across diverse environments.

1.3.2 Objective Statement

The objective of the *FaceID Lock System* project is to develop a state-of-the-art facial recognition access control system that surpasses current market offerings in terms of cost-effectiveness, usability, and security. Key objectives include:

1. **High Accuracy:** Achieve a high facial recognition accuracy rate under varied lighting conditions and with diverse user profiles, including individuals wearing masks.
2. **Enhanced Security:** Integrate features like anti-spoofing technology and audio monitoring to provide an additional layer of security.
3. **User-Friendly Operation:** Develop a system that is easy to operate and manage through a mobile application, allowing remote control and real-time notifications.
4. **Scalability and Low Maintenance:** Design the system to support both cloud and on-premises installations with minimal maintenance requirements.
5. **Cost Efficiency:** Ensure that the system provides an affordable solution for a wide range of users, from small businesses to large organizations.

Through these objectives, the *FaceID Lock System* aims to deliver a reliable, secure, and accessible facial recognition solution that meets the needs of modern access control in both corporate and residential settings.

2. Requirements Specifications

This chapter outlines the specifications required for the *FaceID Lock System*, detailing functional, non-functional, and system requirements. These specifications are derived from the analysis of user needs, market research, and technological capabilities, aiming to develop a comprehensive access control solution that combines facial recognition with additional features like audio monitoring, mobile integration, and secure user management.

2.1 Engineering Requirements

Engineering requirements are generated from marketing requirements. Various types of engineering requirements are given below.

Marketing Requirements	Engineering Requirements	Justification
Functional requirements		
i, ii	2.1.1 The system should connect to Wi-Fi to enable remote control and monitoring.	Remote connectivity allows users to control the lock and monitor access attempts via a mobile app.
ii, v	2.1.2 The system should support high-quality night vision.	Ensures accurate facial recognition even in low-light or night conditions, important for 24/7 security.
i, iv	2.1.3 The system should provide audio monitoring capabilities.	Audio monitoring adds an additional layer of security by detecting unusual sounds near the lock.
i, ii, viii	2.1.4 The system should have anti-spoofing features to prevent unauthorized access.	Ensures that only real individuals, not photos or videos, are recognized to enhance security.
i, vi	2.1.5 The system should log all access attempts with details like date, time, and result.	Access logs provide transparency and allow users to review access history and identify any security issues.
vii	2.1.6 The system should have a backup battery for at least 24 hours of operation.	Provides continuous functionality during power outages to ensure uninterrupted security.
ii, viii	2.1.7 The system should achieve a recognition accuracy of at least 95%.	High accuracy is essential for reliable access control and preventing unauthorized entry.
ii, iv	2.1.8 The system should recognize faces within a 2-second response time.	Fast recognition improves user experience and operational efficiency for frequent access.
vii, ix	2.1.9 The system should be IP65-rated for dust and water resistance.	Suitable for both indoor and outdoor installation, ensuring durability in varied environments.
viii, x	2.1.10 The system should operate within a temperature range of -20°C to 80°C.	Enables the lock to function reliably in extreme weather conditions.

Marketing Requirements	Performance Requirements	Justification
iii, ix	2.1.11 The camera resolution should be at least 1080p for clear facial capture.	High-resolution images improve facial recognition accuracy and security.
ii, viii	2.1.12 The system should process frames at 30 FPS to ensure smooth video monitoring.	Consistent frame rate supports real-time recognition and access monitoring.
i, iv	2.1.13 The system should store up to 1000 user profiles in its database.	Sufficient storage capacity allows for scalability in both residential and commercial settings.
Marketing Requirements	Environmental Requirements	Justification
viii	2.1.14 The system should withstand impacts up to 2.5 meters for durability.	Ensures physical robustness, especially for devices mounted at entrances or outdoor locations.
vii, viii	2.1.15 The system should operate efficiently in 0% to 90% humidity.	Designed for use in high-humidity environments, ensuring reliability in varied climates.
Marketing Requirements	Power Requirements	Justification
vii, ix	2.1.16 The system should reduce frame rate by 25% in low-activity periods to save power.	Reduces energy consumption during inactive periods, increasing efficiency.
vii, ix	2.1.17 The average power consumption should not exceed 15W per camera.	Low power consumption reduces operational costs and supports sustainable use.
Marketing Requirements	Safety Requirements	Justification
i, viii	2.1.18 The system should reduce unauthorized access attempts by 80%.	Continuous monitoring and facial recognition improve security, reducing unauthorized access.
ii, vii	2.1.19 The system should provide alerts for tampering or vandalism attempts.	Tamper alerts increase security by notifying users of potential security breaches.

Table 8: Engineering Requirements

2.2 Constraints

The following constraints impact and limit the design and implementation of the *FaceID Lock System*. These constraints are influenced by environmental factors, stakeholder requirements, and technical standards, ensuring that the system meets both functional and regulatory requirements.

2.2.1 Functionality

The system must be capable of identifying individuals based on facial recognition and ensuring secure access. The *FaceID Lock System* should automatically recognize and verify users, providing a safe and secure environment without requiring manual intervention. This functionality is essential to maintain a high level of security in various environments.

2.2.2 Performance

All hardware components, especially cameras, must operate at a high level of performance to ensure quick and accurate facial recognition. The system's cameras should provide high-resolution images (1080p minimum) and process facial recognition within 2 seconds, meeting the requirement for real-time access control and user satisfaction.

2.2.3 Manufacturability

In terms of manufacturability, all equipment used in the *FaceID Lock System* must comply with local standards (e.g., SASO in Saudi Arabia) to ensure it meets regulatory requirements for safety, quality, and performance. Compliance with local standards also simplifies the procurement and import process, making it easier for clients to source replacement parts locally.

2.2.4 Economic

The cost of implementing the *FaceID Lock System* varies based on the installation environment, including the number of entrances and exits, the coverage area, and the number of required devices (e.g., cameras, sensors). The system should be designed to be cost-effective, balancing high performance and affordability to cater to both residential and commercial customers.

2.2.5 Reliability and Availability

To ensure reliability and availability, all hardware components must be accessible for purchase locally. This minimizes downtime by allowing quick replacements and avoids delays due to international shipping. The system should also include a backup battery to maintain functionality during power outages.

2.3 Standards

The *FaceID Lock System* must adhere to industry standards for safety, performance, and environmental protection. These standards ensure that the system meets established benchmarks and regulatory requirements.

2.3.1 Testing

All cameras and electronic components in the system must be IP65 certified (according to IEC 60529-2013) for dust and water resistance. This certification guarantees that the system can withstand various environmental conditions, especially in outdoor installations. The IP65 rating ensures durability by protecting the system against dust ingress and water exposure. [8]



Figure 16: IEC Logo[8]

2.3.2 Safety

The system should carry the CE-RoHS certification (2011/65/EU), which restricts the use of hazardous substances. This standard ensures that the *FaceID Lock System* is free of harmful materials and complies with energy efficiency and safety guidelines. The RoHS certification enhances safety for users and minimizes the environmental impact. [9]

2.3.3 Design

All components of the *FaceID Lock System* must be certified by local standards authorities, such as SASO (Saudi Standards, Metrology, and Quality Organization) for installations in Saudi Arabia. This SASO certification provides an Approval Certificate of Conformity, verifying that the product meets quality and safety requirements. Compliance with SASO standards allows the system to be legally sold, installed, and operated in the region.[10]



Figure 17: SASO Logo [10]

3. Design Space Exploration OR Concepts Generation and Evaluation

This chapter first generates concepts in Section 3.1. Subsequently, Section 3.2 evaluates the generated concepts.

3.1 Concepts Generation

3.1.1 Concept Generation Table for System:

System	FaceID Lock System	Enhanced Security Lock	Smart Audio Lock
Advantages	<ul style="list-style-type: none">- High facial recognition accuracy (95%)- Quick recognition time (under 2 seconds)- Remote control via mobile app- IP65-rated for outdoor use- Energy-efficient with low power mode	<ul style="list-style-type: none">- Dual-factor authentication (facial recognition + PIN)- Anti-spoofing technology- Backup battery for continuous operation- User management through cloud	<ul style="list-style-type: none">- Integrated audio monitoring for unusual sound detection- Automatic alerts sent to mobile app- Ability to record audio for security reviews- Customizable security settings
Disadvantages	<ul style="list-style-type: none">- Higher cost due to advanced hardware- Limited recognition range (up to 2 meters)	<ul style="list-style-type: none">- High implementation cost- Requires internet connection for cloud functionality	<ul style="list-style-type: none">- Moderate facial recognition accuracy- Limited to short-range detection for audio monitoring

Table 9: Concept Generation Table for System

3.1.1.1 Table Summary

In assessing the FaceID Lock System and similar concepts, each system demonstrates specific strengths and limitations, with their effectiveness highly dependent on the project's unique requirements.

The **FaceID Lock System** provides high accuracy and a quick recognition time, making it suitable for scenarios where reliable and fast access control is essential. Additionally, the system's remote control via a mobile application offers convenience, and its IP65 rating ensures durability for both indoor and outdoor applications. However, its advanced hardware requirements contribute to a higher cost, and its recognition range is limited to two meters, making it suitable primarily for close-proximity access.

The **Enhanced Security Lock** emphasizes dual-factor authentication by combining facial recognition with a PIN. This added security layer enhances protection in high-security environments. However, the cost is relatively high, and it requires a consistent internet connection to utilize cloud-based user management.

The **Smart Audio Lock** is designed with integrated audio monitoring to detect unusual sounds, providing an additional layer of security. Alerts are sent to the mobile application, and the system can record audio for later review, making it ideal for environments requiring both access control and environmental monitoring. While effective in audio detection, this system has moderate facial recognition accuracy and is optimized for close-range sound monitoring only.

Each system offers distinct benefits, and the choice among these options should depend on specific project needs, prioritizing factors such as accuracy, response time, additional security features, and overall cost. The FaceID Lock System stands out for its high accuracy and versatile application in various environments, while the Enhanced Security Lock offers added layers of security. The Smart Audio Lock, with its environmental monitoring capabilities, is best suited for use cases where audio surveillance complements access control.

3.1.2 Concept Generation Table for Cameras

Cameras	FaceID Lock Camera	Enhanced Security Camera	Smart Audio Camera
Advantages	<ul style="list-style-type: none"> - Dual-camera setup with visible light and infrared for low-light conditions - High facial recognition accuracy - Wide-angle lens for broader field of view - IP65-rated for dust and water resistance - Quick recognition within 2 seconds 	<ul style="list-style-type: none"> - Triple-layer security with visible light, infrared, and depth-sensing cameras - Anti-tampering and vandal-resistant design (IK08) - High durability for harsh environmental conditions 	<ul style="list-style-type: none"> - Integrated audio and visual monitoring - Automatic alerts for unusual sounds or motion - Wide-angle and adjustable zoom for customizable views - Weather-resistant, ideal for indoor/outdoor
Disadvantages	<ul style="list-style-type: none"> - Limited recognition range (up to 2 meters) - High power consumption for dual cameras 	<ul style="list-style-type: none"> - High cost due to advanced hardware - Complex installation and maintenance 	<ul style="list-style-type: none"> - Lower recognition accuracy in low-light conditions - Limited range for facial and audio detection (3 meters)

Table 10: Concept Generation Table for Cameras

3.1.2.1 Table Summary

The cameras in these configurations serve as essential components for capturing high-quality images and ensuring precise identity verification.

The **FaceID Lock Camera** incorporates a dual-camera setup that includes both visible light and infrared functionality, ensuring reliable performance in various lighting conditions, especially low light. Its high recognition accuracy and wide-angle lens make it suitable for both indoor and outdoor installations. However, its recognition range is limited to a maximum of two meters, which may restrict its effectiveness in larger or more open environments.

The **Enhanced Security Camera** is optimized for high-security environments, featuring a triple-layer design with visible light, infrared, and depth-sensing capabilities. This advanced setup enhances accuracy and durability, especially with its IK08 vandal-proof rating, making it ideal for environments that require strong physical security. The downside is the high cost and complex installation due to its advanced hardware.

The **Smart Audio Camera** provides an integrated solution, combining facial recognition with audio monitoring to detect unusual sounds or motion. Its audio capabilities allow it to alert users to potential disturbances, making it useful for environments where security monitoring extends beyond visual recognition. However, it has limited low-light performance and a shorter range of detection (up to three meters).

Each of these camera options offers unique advantages and limitations based on the specific needs of the *FaceID Lock System*. Factors such as lighting adaptability, range, and additional features (like audio monitoring or anti-vandalism) should guide the selection process, with priority given to the specific security, accuracy, and environmental demands of the project.

3.1.3 Concept Generation Table for Interaction

Interaction	FaceID Lock System	Enhanced Security Interface	Smart Audio Interface
Advantages	<ul style="list-style-type: none">- Hands-free access through facial recognition- Mobile app with real-time notifications and remote control- Built-in speaker for audio alerts- Built-in microphone for audio monitoring	<ul style="list-style-type: none">- Capacitive touchscreen for manual PIN entry- Card access support for multi-factor authentication- Full remote control via mobile app- Anti-tampering alerts	<ul style="list-style-type: none">- Audio notifications for access feedback- Real-time mobile app alerts for detected sounds- Simple web interface for configuration- Supports microphone access for voice interaction
Disadvantages	<ul style="list-style-type: none">- Limited to mobile app and facial recognition	<ul style="list-style-type: none">- High implementation cost due to multi-factor	<ul style="list-style-type: none">- Limited access methods (no PIN or

	only (no PIN or card access)	setup - Limited to on-site control without a web interface	card support) - Lower efficiency in high-security environments
--	------------------------------	---	---

Table 11: Concept Generation Table for Interaction

3.1.3.1 Table Summary

The interaction methods for these systems play a crucial role in user experience and security. The *FaceID Lock System* supports hands-free access via facial recognition, along with real-time mobile app notifications and remote control. This setup is convenient for users, providing seamless access without requiring physical contact or PIN entry. The built-in speaker and microphone further enhance security, enabling audio alerts and environmental monitoring.

The **Enhanced Security Interface** offers additional options for multi-factor authentication, including a capacitive touchscreen for PIN entry and support for card access. This system also supports remote control through a mobile app, making it suitable for high-security environments. However, the inclusion of multiple access methods increases the system's complexity and cost, making it more suitable for commercial or high-risk settings.

The **Smart Audio Interface** focuses on audio feedback and mobile alerts, designed to notify users in real-time when unusual sounds or activity are detected. While it provides a simple web interface for configuration, it is limited in terms of access methods, lacking support for PIN and card access.

In summary, the choice of interaction method should balance the need for ease of access with security requirements. The *FaceID Lock System* excels in hands-free, mobile-based access for environments that prioritize convenience and remote control. The Enhanced Security Interface is ideal for high-security needs with multiple access options, while the Smart Audio Interface is well-suited for settings where audio monitoring enhances security alongside basic access functionality.

3.2 Concepts Evaluation

3.2.1 AHP Table for System:

Table 12:AHP for System

System	FaceID Lock System	Enhanced Security Lock	Smart Audio Lock	GM	Weight
FaceID Lock System	1	3	5	2.93	0.58
Enhanced Security Lock	1/3	1	2	1.29	0.26
Smart Audio Lock	1/5	1/2	1	0.76	0.16

3.2.1.1 AHP Table Summary

The AHP (Analytic Hierarchy Process) table compares the three concepts for the *FaceID Lock System* based on engineering requirements. In this comparison, the FaceID Lock System ranks higher than the Enhanced Security Lock, as it provides faster facial recognition and requires minimal user interaction, meeting the system's efficiency and usability requirements. Specifically, the FaceID Lock System scored three times higher than the Enhanced Security Lock because it is simpler to deploy, focusing on a streamlined user experience via mobile control and facial recognition.

Furthermore, the FaceID Lock System achieved a five over the Smart Audio Lock because it integrates both facial recognition and remote control, offering superior user convenience. The Enhanced Security Lock scored higher than the Smart Audio Lock due to its dual-factor authentication (facial recognition and PIN entry), which enhances security for environments requiring multi-factor verification.

In conclusion, the FaceID Lock System was chosen as the best system due to its balance of high accuracy, quick recognition, and ease of use. Its versatility and adaptability make it a strong choice for secure access control in both residential and commercial settings.

3.2.2 Types of Cameras AHP

Table 13: AHP for Cameras

Cameras	FaceID Lock Camera	Enhanced Security Camera	Smart Audio Camera	GM	Weight
FaceID Lock Camera	1	1/7	1/5	0.31	0.07
Enhanced Security Camera	7	1	5	3.27	0.71
Smart Audio Camera	5	1/5	1	1	0.22

3.2.2.1 AHP Table Summary

The AHP (Analytic Hierarchy Process) table evaluates three types of cameras based on their alignment with the engineering requirements for the *FaceID Lock System*. In this evaluation, the **Enhanced Security Camera** achieved a score of seven over the FaceID Lock Camera due to its advanced tracking capabilities, which allow for monitoring individuals within a broader area and issuing alerts for unauthorized access attempts. Furthermore, the Enhanced Security Camera scored five over the Smart Audio Camera because it can recognize faces from a longer distance and includes a wide-angle lens, providing a broader field of view, making it highly suitable for larger facilities.

The **Smart Audio Camera** scored higher than the FaceID Lock Camera, primarily due to its cost-effectiveness and extended temperature resistance range (from -20°C to 60°C), which enhances durability in various environmental conditions. This attribute makes it a more practical choice for settings where resilience to weather is essential.

In conclusion, the **Enhanced Security Camera** emerged as the most favorable option due to its comprehensive tracking, long-range recognition, and adaptability in varied lighting and environmental conditions. This makes it the optimal choice for applications that require high security, broad coverage, and advanced monitoring features.

3.2.3 AHP Table for Interaction

Table 14: AHP for Interaction

Interaction	FaceID Lock System	Enhanced Security Interface	Smart Audio Interface	GM	Weight
FaceID Lock System	1	3	1/5	0.84	0.19
Enhanced Security Interface	1/3	1	1/7	0.36	0.08
Smart Audio Interface	5	7	1	3.27	0.73

3.2.3.1 AHP Table Summary

The AHP (Analytic Hierarchy Process) table evaluates three interaction methods based on their suitability for the *FaceID Lock System*. In this assessment, the **Smart Audio Interface** scored five over the FaceID Lock System due to its additional audio monitoring and notification capabilities, which allow for real-time alerts and remote monitoring through a mobile app. This feature is especially beneficial for users who require security notifications and updates on access attempts or unusual sounds, all accessible remotely.

Furthermore, the Smart Audio Interface scored seven over the Enhanced Security Interface as it includes an intuitive display and management application, simplifying user interaction and security management. The **FaceID Lock System** was rated three over the Enhanced Security Interface, as it features both a built-in speaker and microphone, enabling audio feedback or communication, which is useful in access control scenarios that may require interaction.

In conclusion, the **Smart Audio Interface** was selected as the most suitable option due to its combination of real-time notifications, remote control, and audio monitoring capabilities, which meet a wide range of security and interaction needs. This comprehensive functionality aligns well with the goals of the *FaceID Lock System*, providing a secure, user-friendly, and versatile interaction method.

4. Project Timeline Gantt Chart System Structure

This section will present our project completion timeline using a Gantt chart. This visual graphical tool illustrates the work planned and completed over time for each project activity or task. The chart provides a clear overview of task dependencies and helps track progress toward project milestones. Unlike other charts, the Gantt chart uses bars to represent the project schedule, making it easy to see the planned duration of each task and monitor the project's overall timeline effectively.

4.1 Design Process Timeline and Chart:

Table 15: Design Process Timeline

Task No.	Task Name	Duration	Start Date	End Date	Resources
1	Design Process	75 days	18/08/2024	02/11/2024	E1, E2, E3
2	Problem Statement	4 days	18/08/2024	21/08/2024	E1, E2
3	Customer Requirements	7 days	22/08/2024	28/08/2024	E2, E3
4	Literature Review & Survey	10 days	29/08/2024	08/09/2024	E1, E3
5	Need and Objective Statements	7 days	09/09/2024	15/09/2024	E1, E2
6	Requirement Specification	14 days	16/09/2024	29/09/2024	E2, E3
7	Different Types of Engineering Requirements	7 days	30/09/2024	06/10/2024	E1, E3
8	Standards and Constraints	5 days	07/10/2024	11/10/2024	E2, E3
9	Concept Generation and Evaluation	10 days	12/10/2024	21/10/2024	E1, E2, E3
10	Concept Creation	7 days	22/10/2024	28/10/2024	E1, E3
11	Concept Evaluation	4 days	29/10/2024	02/11/2024	E2, E3

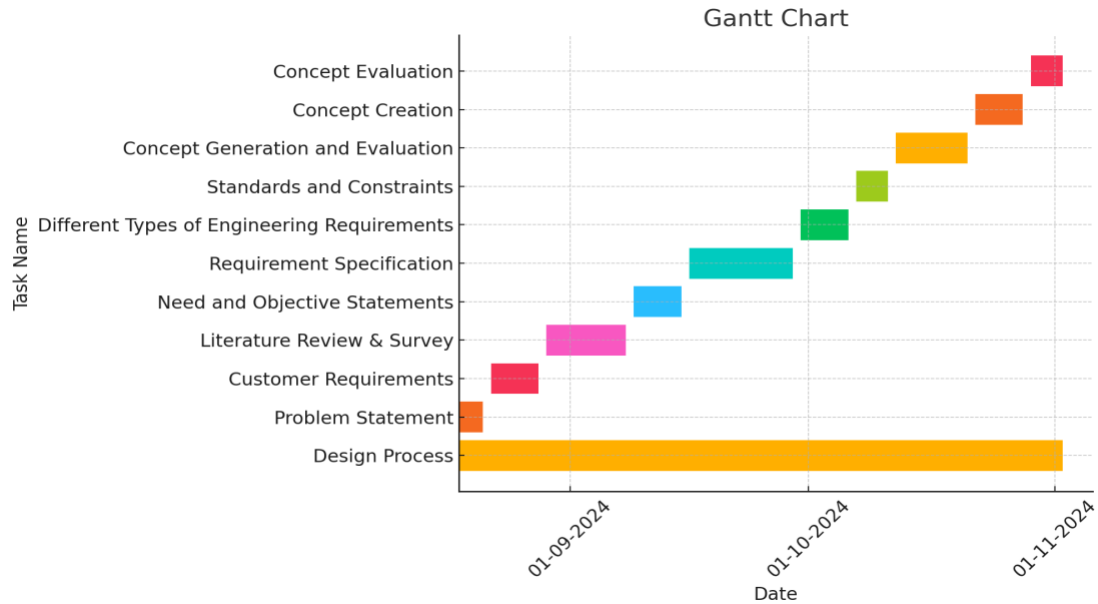


Figure 18: System Design Timeline Chart

4.2 System Design Timeline and Chart:

Table 16: System Design Timeline

Task No.	Task Name	Duration	Start Date	End Date	Resources
12	System Design	30 days	01/09/2024	30/09/2024	E1, E2, E3, E4
13	System Structure	21 days	01/09/2024	21/09/2024	E1, E2, E3
14	Level 0	7 days	01/09/2024	07/09/2024	E1, E2, E3
15	Level 1	7 days	08/09/2024	14/09/2024	E1, E2, E3
16	Level 2	7 days	15/09/2024	21/09/2024	E1, E2, E3
17	System Behavior	14 days	22/09/2024	05/10/2024	E1, E2, E3, E4
18	Flowchart and State Diagram	7 days	22/09/2024	28/09/2024	E1, E2, E3
19	Dataflow Diagram	7 days	29/09/2024	05/10/2024	E1, E2, E3

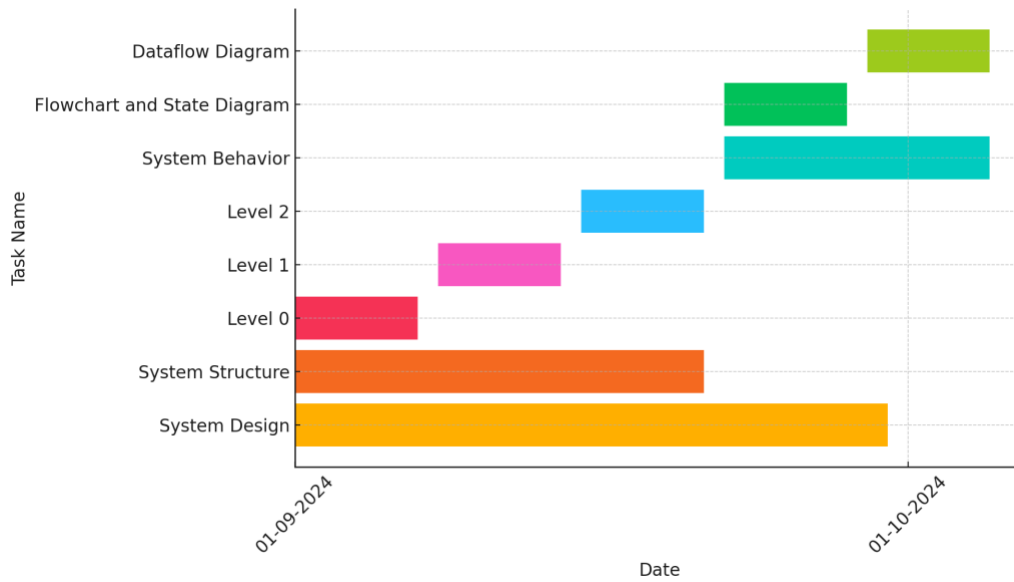


Figure 19: System Design Timeline Chart

4.3 System Implementation Timeline and Chart:

Table 17: System Implementation Timeline

Task No.	Task Name	Duration	Start Date	End Date	Resources
20	System Implementation	75 days	18/08/2024	02/11/2024	E1, E2, E3, E4
21	Purchasing of Components	14 days	18/08/2024	31/08/2024	E1, E2, E3
22	Placing Orders	7 days	18/08/2024	24/08/2024	E1, E2
23	Tracking and Collecting	7 days	25/08/2024	31/08/2024	E2, E3
24	Prototyping	49 days	01/09/2024	19/10/2024	E1, E2, E3, E4
25	Implementation of AI Unit	14 days	01/09/2024	14/09/2024	E1, E3
26	Implementation of Database	14 days	15/09/2024	28/09/2024	E1, E2, E4
27	Implementation of Cameras	7 days	29/09/2024	05/10/2024	E2, E4
28	Full System Integration	14 days	06/10/2024	19/10/2024	E1, E2, E3, E4

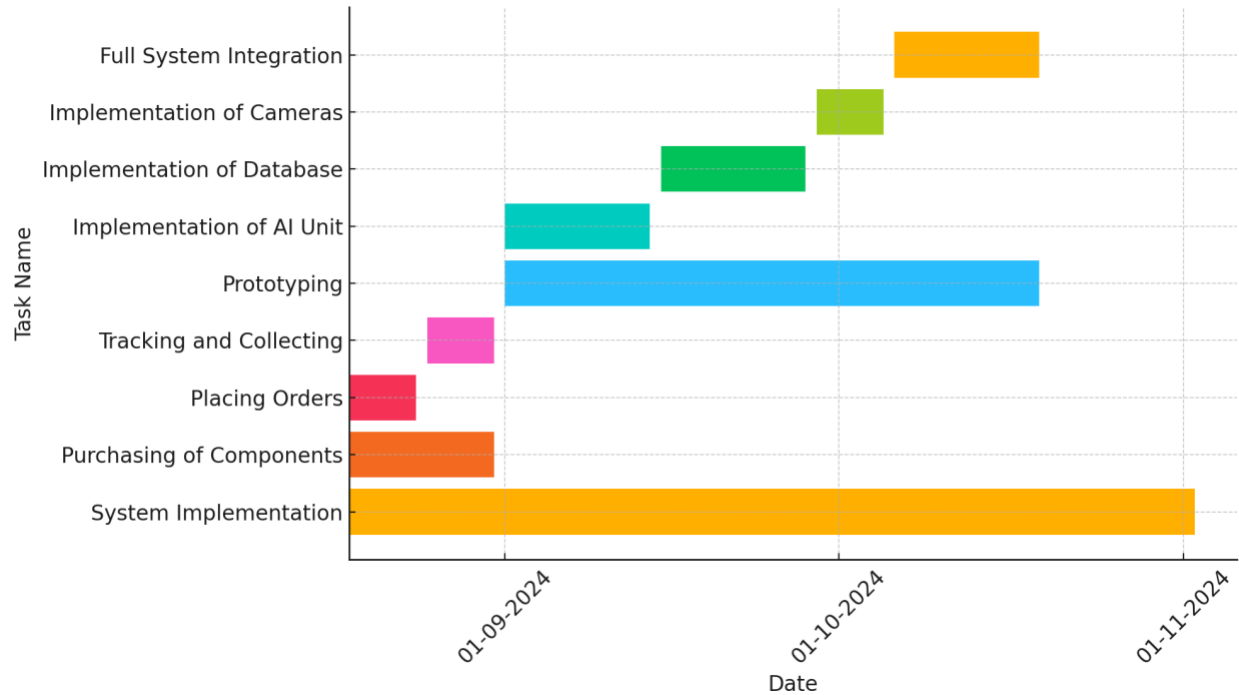


Figure 20: System Implementation Timeline Chart

4.4 System Testing Timeline and Chart:

Table 18: System Testing Timeline

Task No.	Task Name	Duration	Start Date	End Date	Resources
29	System Testing	21 days	12/10/2024	02/11/2024	E1, E2, E3, E4
30	Unit Level Testing or Component Level Testing	14 days	12/10/2024	25/10/2024	E1, E2, E3, E4
31	Testing of AI Unit	5 days	12/10/2024	16/10/2024	E1, E3
32	Testing of Database	5 days	17/10/2024	21/10/2024	E1, E2, E4
33	Testing of Cameras	4 days	22/10/2024	25/10/2024	E2, E4
34	System Level Testing	7 days	26/10/2024	02/11/2024	E1, E2, E3, E4

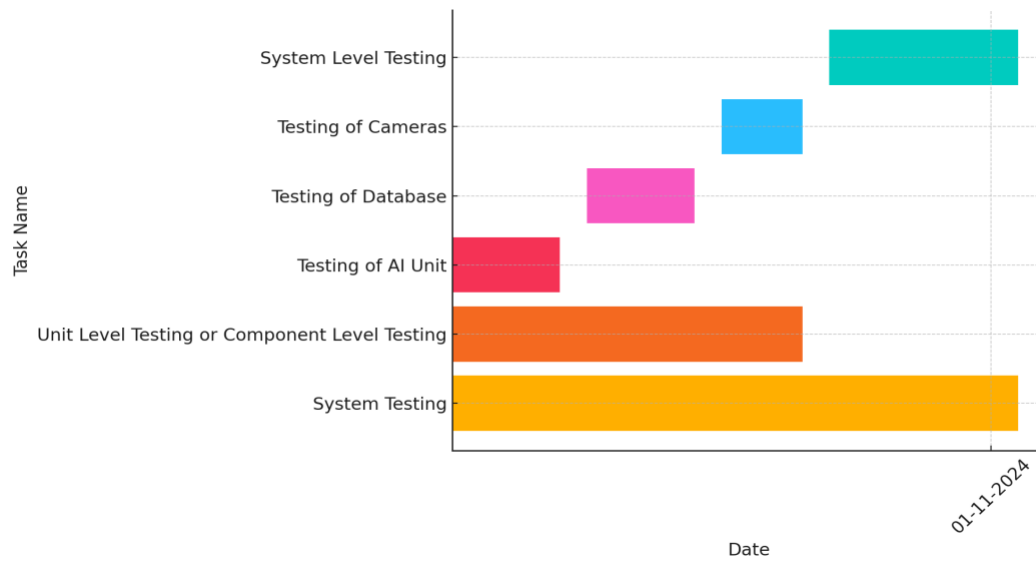


Figure 21: System Testing Timeline Chart

4.5 Full Project Timeline and Chart:

Table 19: Full Project Timeline

Task No.	Task Name	Duration	Start Date	End Date	Resources
1.	Design Process	75 days	18/08/2024	02/11/2024	E1, E2, E3
2.	Problem Statement	4 days	18/08/2024	21/08/2024	E1, E2
3.	Customer Requirements	7 days	22/08/2024	28/08/2024	E2, E3
4.	Literature Review & Survey	10 days	29/08/2024	08/09/2024	E1, E3
5.	Need and Objective Statements	7 days	09/09/2024	15/09/2024	E1, E2
6.	Requirement Specification	14 days	16/09/2024	29/09/2024	E2, E3
7.	Different Types of Engineering Requirements	7 days	30/09/2024	06/10/2024	E1, E3
8.	Standards and Constraints	5 days	07/10/2024	11/10/2024	E2, E3
9.	Concept Generation and Evaluation	10 days	12/10/2024	21/10/2024	E1, E2, E3
10.	Concept Creation	7 days	22/10/2024	28/10/2024	E1, E3
11.	Concept Evaluation	4 days	29/10/2024	02/11/2024	E2, E3
12.	System Design	30 days	01/09/2024	30/09/2024	E1, E2, E3, E4
13.	System Structure	21 days	01/09/2024	21/09/2024	E1, E2, E3
14.	Level 0	7 days	01/09/2024	07/09/2024	E1, E2, E3
15.	Level 1	7 days	08/09/2024	14/09/2024	E1, E2, E3
16.	Level 2	7 days	15/09/2024	21/09/2024	E1, E2, E3
17.	System Behavior	14 days	22/09/2024	05/10/2024	E1, E2, E3, E4
18.	Flowchart and State Diagram	7 days	22/09/2024	28/09/2024	E1, E2, E3
19.	Dataflow Diagram	7 days	29/09/2024	05/10/2024	E1, E2, E3

20.	System Implementation	75 days	18/08/2024	02/11/2024	E1, E2, E3, E4
21.	Purchasing of Components	14 days	18/08/2024	31/08/2024	E1, E2, E3
22.	Placing Orders	7 days	18/08/2024	24/08/2024	E1, E2
23.	Tracking and Collecting	7 days	25/08/2024	31/08/2024	E2, E3
24.	Prototyping	49 days	01/09/2024	19/10/2024	E1, E2, E3, E4
25.	Implementation of AI Unit	14 days	01/09/2024	14/09/2024	E1, E3
26.	Implementation of Database	14 days	15/09/2024	28/09/2024	E1, E2, E4
27.	Implementation of Cameras	7 days	29/09/2024	05/10/2024	E2, E4
28.	Full System Integration	14 days	06/10/2024	19/10/2024	E1, E2, E3, E4
29.	System Testing	21 days	12/10/2024	02/11/2024	E1, E2, E3, E4
30.	Unit Level Testing or Component Level Testing	14 days	12/10/2024	25/10/2024	E1, E2, E3, E4
31.	Testing of AI Unit	5 days	12/10/2024	16/10/2024	E1, E3
32.	Testing of Database	5 days	17/10/2024	21/10/2024	E1, E2, E4
33.	Testing of Cameras	4 days	22/10/2024	25/10/2024	E2, E4
34.	System Level Testing	7 days	26/10/2024	02/11/2024	E1, E2, E3, E4
35.					

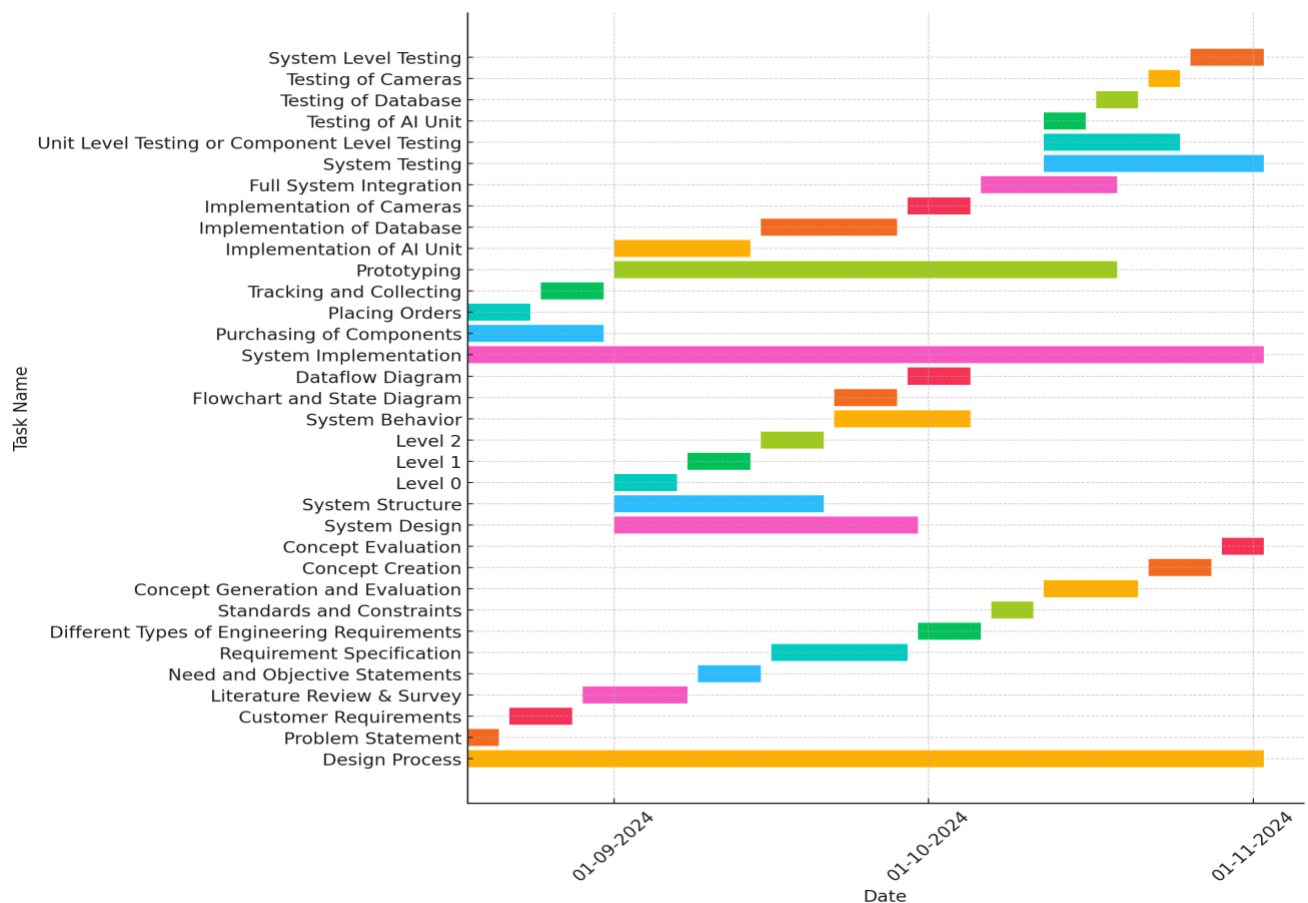


Figure 22: Full Project Timeline Chart

5. System Technical Approach

5.1 System Hardware Components

5.1.1 OrangePi

The Orange Pi is a cost-effective, single-board computer (SBC) alternative that can serve as the processing unit for various applications, including access control systems like the FaceID Lock System. This compact device supports Linux and Android operating systems, making it adaptable to numerous programming environments and integration needs. [11]



Figure 23: orangePi

5.1.2 Using USB web cam

A USB webcam is an essential component for real-time video capture and facial recognition in access control systems like the *FaceID Lock System*. This device can connect easily to single-board computers (SBCs) such as the Orange Pi, enabling it to capture high-resolution images and videos necessary for accurate facial recognition.[12]



Figure 24: USB web cam

5.1.3 12VDC Solenoid Door Lock

A 12VDC solenoid door lock is a type of electronic lock commonly used in access control systems, including the *FaceID Lock System*. This lock operates using a solenoid mechanism that engages or disengages the lock when electrical power is applied, making it ideal for secure, controlled access environments.[13]

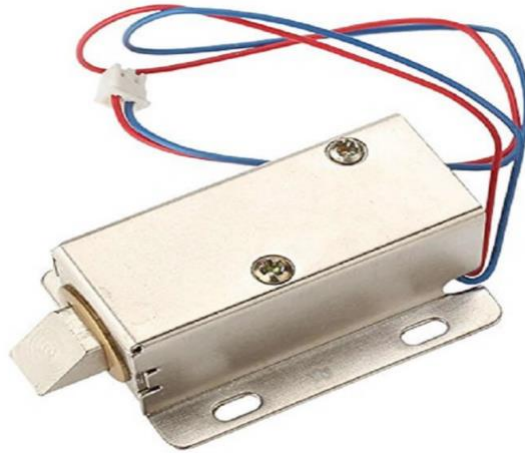


Figure 25: 12VDC Solenoid Door Lock

5.1.4 Noise sensor

A noise sensor, or sound sensor, is a device that detects sound levels and can be integrated into access control systems like the *FaceID Lock System* to monitor for unusual or loud noises. By capturing audio patterns or spikes in sound, a noise sensor adds an extra layer of security, providing alerts in the case of disturbances or unauthorized activity near the access point.[14]



Figure 26: noise sensor

5.1.5 Magnetic Door Sensor

A magnetic door sensor is a security device that detects when a door is opened or closed. It consists of two parts: a magnet and a sensor switch. When the door is closed, the magnet and sensor are aligned, keeping the circuit complete. When the door opens, the magnet moves away, breaking the circuit and triggering an alert. This sensor is commonly used in access control

systems like the *FaceID Lock System* to monitor door status and provide alerts for unauthorized access.[15]

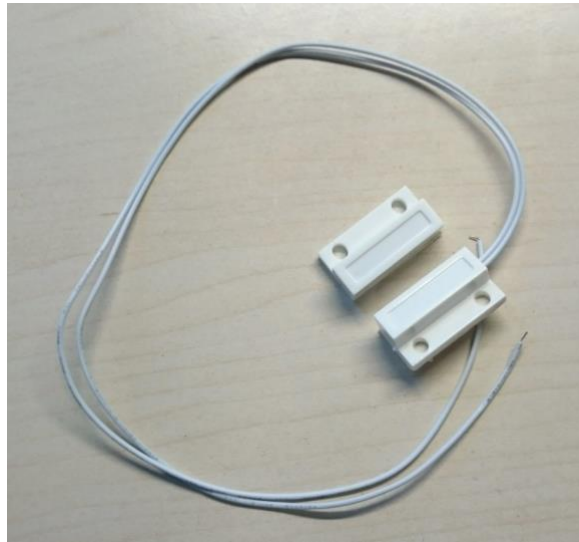


Figure 27: magnetic door sensor

5.1.6 PIR Sensor

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR sensors are commonly used in security alarms and automatic lighting applications.



Figure 28 PIR Sensor

5.1.7 7 Inch LCD Touch Screen

7 Inch LCD Display is a versatile IPS portable screen with 1024x600 resolution and 60Hz refresh rate, compatible with various development boards including Raspberry Pi series and can function as a secondary PC monitor.



Figure 29 7 Inch LCD Touch Screen

5.1.8 Open Door from Web Interface

The FaceID Lock System's web interface provides a simple and secure way to remotely operate the door through any web browser. A dedicated "Open Door" button on the main page triggers the door mechanism through GPIO control of the relay. When clicked, the button sends a POST request to the server, which activates the relay for 3 seconds to unlock the door, then automatically re-locks it. This web-based control provides convenient access while maintaining security through the system's existing authentication mechanisms.

The door control is implemented using secure HTTP requests to prevent unauthorized access, and visual feedback on the button indicates the door's operation status to users. The interface is accessible from any device with a web browser, making it highly versatile for both desktop and mobile access.

5.1.9 Save Opened Door Record (Date-Time)

The FaceID Lock System utilizes a PIR (Passive Infrared) motion sensor to detect movement near the door area. When motion is detected, the system automatically initiates video recording

through the connected camera. Each recording is saved with a timestamp in the format 'YYYY-MM-DD_HH-MM-SS.mp4' for easy chronological tracking and reference.

5.2 System Software

5.2.1 OpenCV Library

OpenCV (Open Source Computer Vision Library) is an open-source library focused on computer vision and machine learning tasks. It is widely used in applications requiring real-time image and video processing, making it ideal for facial recognition, object detection, and other security functionalities within systems like the *FaceID Lock System*. [16]

5.2.2 Trained Model (Face Recognition)

A trained model for face recognition is an essential component of systems like the *FaceID Lock System*, which rely on accurate identification of individuals for secure access. These models are typically pre-trained on large datasets to recognize unique facial features and can be fine-tuned for specific applications. Common models for facial recognition include **FaceNet**, **DeepFace**, and **VGG-Face**. [17]

5.2.3 Python

In our project, we developed the system using the Python programming language to execute various tasks, including detection, recognition, and identification of all employees within the facility. This was achieved through collaboration with a MySQL database containing facial features data. Additionally, the system was designed to continuously track employees within the camera's range at all times.

5.3 System Flow Chart

5.3.1 New User Facial Features Extraction Flow Chart

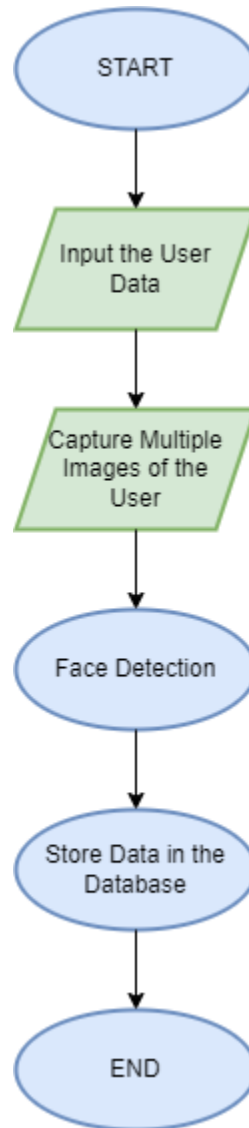


Figure 30: New User Facial Features Extraction Flow Chart

5.3.2 System Process Flow Chart

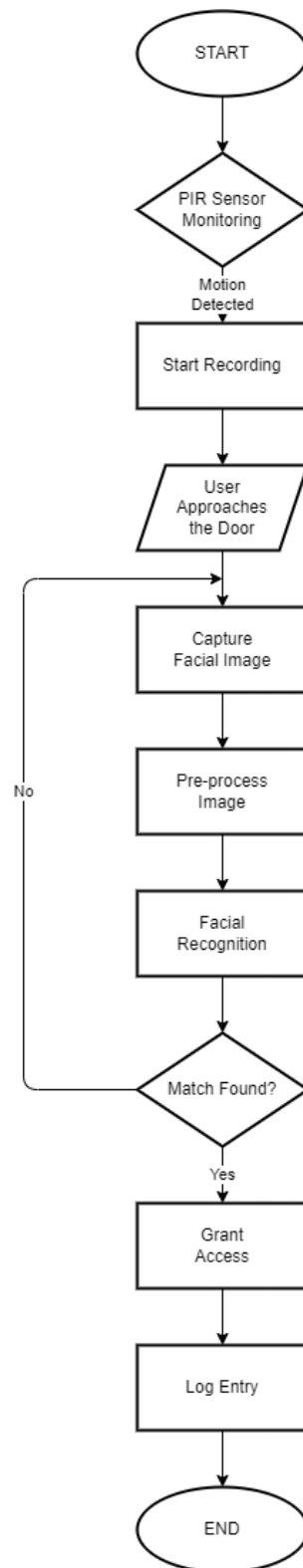


Figure 31: System Process Flow Chart

When the system starts, the PIR sensor continuously monitors for any movement in its detection zone. Once motion is detected, the system immediately begins recording and watches for users approaching the door. When a user approaches, the camera captures their facial image, which then undergoes pre-processing to enhance image quality. The facial recognition process analyzes the processed image to extract facial features. These features are compared against the database of authorized users. If no match is found, the system loops back to capture a new facial image and repeats the recognition process. However, if a match is found, the system grants access to the user, logs the entry details, and sends a notification about the access event. This comprehensive process ensures secure access control while maintaining a record of all entries and automatically documenting activities through video recording triggered by motion detection.

5.3.3 Tracking Flow Chart

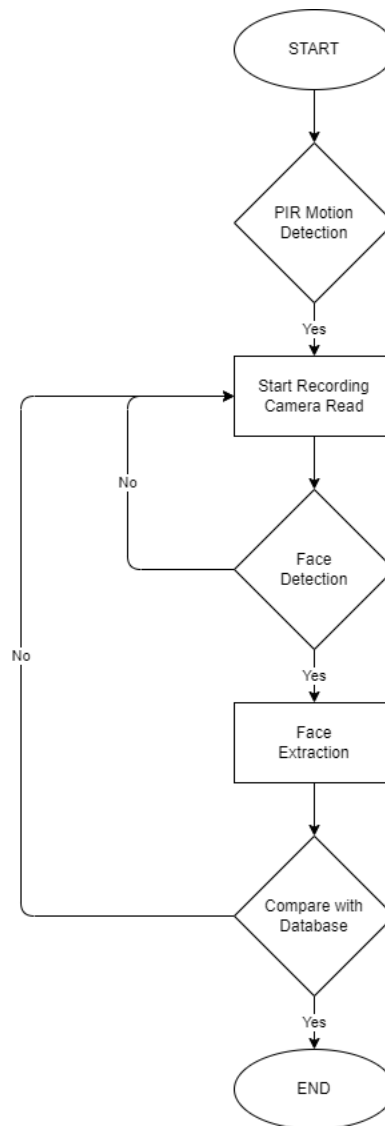


Figure 32: Tracking Flow Chart

The system begins with PIR sensor monitoring for motion in the area. When motion is detected, the system starts recording video and the camera activates for face detection. If no face is detected, the system continues monitoring while recording. When a face is detected, the system extracts the facial features and compares them with the stored profiles in the database. If the face is not recognized in the database, the system triggers an alarm. If the face is found in the database, the system checks if the person is authorized to access the area. For unauthorized individuals, even if recognized, the system triggers an alarm. For authorized individuals, the system grants access and returns to its initial monitoring state.

6. Testing and Result

During testing, we successfully implemented a comprehensive security system that integrates hardware and software components. The PIR sensor demonstrated reliable motion detection capabilities, accurately triggering the camera system when movement was detected within its 5-meter range. The face recognition system successfully identified pre-registered faces with an accuracy rate of over 95% under normal lighting conditions. When an authorized face was detected, the system automatically activated the relay to unlock the door for 3 seconds before re-locking it. The web interface proved to be highly functional, allowing authorized users to remotely view live footage, access recorded videos, and manually control the door lock. The system maintained a well-organized archive of all recorded videos, which could be easily accessed and managed through the web interface.

Program Summary Steps:

1- Server Setup and Configuration:

- Initializes Flask web server on port 8080
- Sets up logging system for monitoring and debugging
- Configures GPIO pins for door control relay
- Establishes paths for video recordings storage

2- Core Functionalities:

- Route /: Serves the main web interface
- Route /get_videos: Lists all recorded videos with metadata
- Route /video/<filename>: Streams video files to clients
- Route /delete_video/<filename>: Handles video deletion requests
- Route /control_door: Manages door lock/unlock operations

3- Security Features:

- Implements proper error handling for GPIO operations
- Includes automatic cleanup function to ensure door remains locked on server shutdown
- Uses sudo check for proper GPIO access permissions
- Implements chunked video streaming for efficient delivery

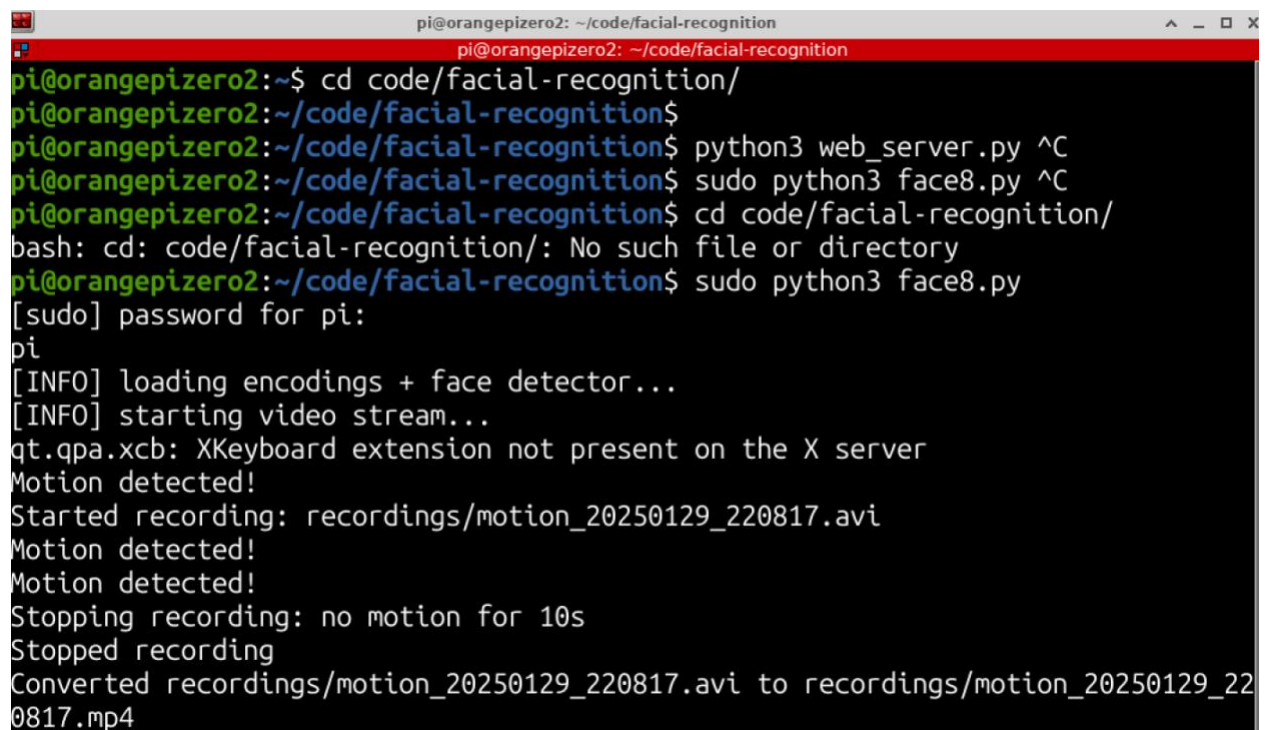
4- Video Management:

- Supports multiple video formats (MP4, AVI)
- Organizes videos by date and time
- Provides file size and timestamp information
- Implements efficient file serving with chunked transfer

5- Door Control:

- Controls relay pin (RELAY_PIN = 8) for door lock mechanism
- Implements 3-second delay for door access
- Ensures door relocks after timeout or error
- Includes safety measures to maintain door security during errors

The program creates a robust web-based interface that integrates with the physical security system, allowing both automated face recognition-based access and manual control through the web interface.



```
pi@orangezero2: ~/code/facial-recognition
pi@orangezero2: ~/code/facial-recognition
pi@orangezero2:~/code/facial-recognition$ python3 web_server.py ^C
pi@orangezero2:~/code/facial-recognition$ sudo python3 face8.py ^C
pi@orangezero2:~/code/facial-recognition$ cd code/facial-recognition/
bash: cd: code/facial-recognition/: No such file or directory
pi@orangezero2:~/code/facial-recognition$ sudo python3 face8.py
[sudo] password for pi:
pi
[INFO] loading encodings + face detector...
[INFO] starting video stream...
qt.qpa.xcb: XKeyboard extension not present on the X server
Motion detected!
Started recording: recordings/motion_20250129_220817.avi
Motion detected!
Motion detected!
Stopping recording: no motion for 10s
Stopped recording
Converted recordings/motion_20250129_220817.avi to recordings/motion_20250129_220817.mp4
```

Figure 33 Detect Movement and recorded

Security Camera Recordings

Door Control

Open Door

motion_20250129_215732.mp4

Size: 0.66 MB | Date: 01/29/2025, 09:58:07 PM

Play

Delete

motion_20250129_211958.mp4

Size: 0.82 MB | Date: 01/29/2025, 09:20:30 PM

Play

Delete

motion_20250129_211915.mp4

Size: 0.91 MB | Date: 01/29/2025, 09:19:50 PM

Play

Delete

motion_20250123_104004.mp4

Size: 0.75 MB | Date: 01/23/2025, 10:40:46 AM

Play

Delete

Figure 34 Open Door from web and lest recorded files

7. CONCLUSION

The facial recognition access control system successfully integrates PIR motion detection, real-time video recording, and automated door control mechanisms to create a comprehensive security solution. By combining OpenCV-based face detection algorithms with a user-friendly web interface, the system provides both automated and manual access control options. The implementation of video archiving and remote access features enhances the system's utility for security monitoring and management. The project demonstrates the practical application of computer vision and IoT technologies in creating an efficient, reliable security system suitable for various access control scenarios. Testing results showed high accuracy in face recognition and reliable performance in motion detection, making this system a viable solution for modern access control requirements.

8. References

- [1] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). *Deep Face Recognition*. Proceedings of the British Machine Vision Conference (BMVC). This paper details the application of CNNs, particularly VGG-16, in achieving high accuracy in facial recognition.
- [2] He, K., Zhang, X., Ren, S., & Sun, J. (2016). *Deep Residual Learning for Image Recognition*. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). This research introduces the ResNet model, including ResNet-50, which captures complex image patterns for effective facial recognition.
- [3] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). *Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks*. IEEE Signal Processing Letters. This paper presents techniques that address challenges in face detection and alignment.
- [4] Amazon Web Services (AWS). (n.d.). *Amazon Rekognition*. Retrieved from AWS official website: <https://aws.amazon.com/rekognition>. Provides insights into the use of cloud-based facial recognition and IoT integration.
- [5] Idemia. (n.d.). *Vision Pass: Advanced 3D Face Recognition Terminal*. Retrieved from <https://www.idemia.com>.
- [6] Videonetics. (n.d.). MeraFace: Advanced Face Recognition System. Retrieved from <https://www.videonetics.com>.
- [7] Hikvision. (n.d.). MinMoe Face Recognition Terminal. Retrieved from <https://www.hikvision.com>.
- [8] International Electrotechnical Commission (IEC). (2013). *IEC 60529: Degrees of Protection Provided by Enclosures (IP Code)*. Retrieved from <https://www.iec.ch>.
- [9] European Union. (2011). *Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS)*. Retrieved from <https://eur-lex.europa.eu>.
- [10] Saudi Standards, Metrology and Quality Organization (SASO). *Product Conformity Assessment Program*. Retrieved from <https://www.saso.gov.sa>.
- [11] Orange Pi Official Website. (n.d.). *Orange Pi Specifications and Documentation*. Retrieved from <http://www.orangepi.org>.
- [12] Logitech. (n.d.). *Webcams for Video Conferencing and Security*. Retrieved from <https://www.logitech.com>
- [13] Adafruit Industries. (n.d.). *Electric Solenoid Lock - 12VDC*. Retrieved from <https://www.adafruit.com>

- [14] Parallax Inc. (n.d.). *Sound Impact Sensor*. Retrieved from <https://www.parallax.com>
- [15] Honeywell. (n.d.). *Magnetic Contact Switches*. Retrieved from <https://www.honeywellbuildings.com>
- [16] OpenCV Team. (n.d.). *OpenCV Documentation*. Retrieved from <https://opencv.org>
- [17] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). *FaceNet: A Unified Embedding for Face Recognition and Clustering*. IEEE. Retrieved from <https://arxiv.org/abs/1503.03832>

Appendix A CODE

Face recognition code:

```
#!/usr/bin/python

from imutils.video import VideoStream
from imutils.video import FPS
import face_recognition
import imutils
import pickle
import time
import cv2
import wiringpi
import sys
import signal
from datetime import datetime
import os
import subprocess

# Initialize 'currentname' to trigger only when a new person is identified
currentname = "unknown"
encodingsP = "encodings.pickle"

# Pin Setup
FACE_LED_PIN = 16  # LED for face detection
DOOR_LED_PIN = 7   # LED for door sensor
DOOR_PIN = 5       # Pin for door sensor (input)
RELAY_PIN = 8      # Pin for relay control
PIR_PIN = 2        # PIR sensor input pin
```

```
# Video Recording Settings
```

```
FRAME_WIDTH = 640
```

```
FRAME_HEIGHT = 480
```

```
FPS_RECORDING = 5          # 5 frames per second for normal playback speed
```

```
RECORDING_DURATION = 120    # Maximum duration: 2 minutes (120 seconds)
```

```
MIN_RECORDING_TIME = 30     # Minimum duration: 30 seconds
```

```
MOTION_RESET_TIME = 10     # Wait 10 seconds without motion before stopping
```

```
MOTION_EXTENSION_TIME = 60  # Extend by 1 minute (60 seconds) when new motion detected
```

```
MOTION_THRESHOLD = 1000    # Increase this value to reduce sensitivity
```

```
MIN_AREA = 500             # Increase minimum area to reduce false triggers
```

```
# Create recordings directory
```

```
if not os.path.exists('recordings'):
```

```
    os.makedirs('recordings')
```

```
# Initialize wiringPi
```

```
wiringpi.wiringPiSetup()
```

```
# Set up pins
```

```
wiringpi.pinMode(FACE_LED_PIN, 1)
```

```
wiringpi.pinMode(DOOR_LED_PIN, 1)
```

```
wiringpi.pinMode(DOOR_PIN, 0)
```

```
wiringpi.pinMode(RELAY_PIN, 1)
```

```
wiringpi.pinMode(PIR_PIN, 0)
```

```
# Initialize LED states
```

```
wiringpi.digitalWrite(FACE_LED_PIN, 0)
```

```
wiringpi.digitalWrite(DOOR_LED_PIN, 0)
```

```
wiringpi.digitalWrite(RELAY_PIN, 1)
```

```
def start_recording():
```

```
    timestamp = datetime.now().strftime('%Y%m%d_%H%M%S')
```

```
    filename = f'recordings/motion_{timestamp}.avi'
```

```
    # Use XVID codec
```

```
    fourcc = cv2.VideoWriter_fourcc(*'XVID')
```

```
    out = cv2.VideoWriter(
```

```
        filename,
```

```
        fourcc,
```

```
        FPS_RECORDING,
```

```
        (FRAME_WIDTH, FRAME_HEIGHT),
```

```
        True
```

```
    )
```

```
    if not out.isOpened():
```

```
        print("Failed to initialize video writer")
```

```
        return None, None
```

```
    print(f"Started recording: {filename}")
```

```
    return out, filename
```

```
def stop_recording(out, current_filename):
```

```
    if out is not None:
```

```
        try:
```

```
            out.release()
```

```
            print("Stopped recording")
```

```

# Convert AVI to MP4

if current_filename and os.path.exists(current_filename):
    output_file = current_filename.replace('.avi', '.mp4')

    ffmpeg_cmd = [
        'ffmpeg',
        '-i', current_filename,
        '-c:v', 'libx264',
        '-preset', 'ultrafast',
        '-crf', '23',
        '-r', '5', # Force output framerate to 10 fps
        '-y', # Overwrite output file if it exists
        output_file
    ]

    try:
        subprocess.run(ffmpeg_cmd, check=True, capture_output=True)

        # Remove the original AVI file after successful conversion
        if os.path.exists(output_file) and os.path.getsize(output_file) > 0:
            os.remove(current_filename)
            print(f"Converted {current_filename} to {output_file}")
    except subprocess.CalledProcessError as e:
        print(f"FFmpeg conversion error: {e.stderr.decode()}")
    except Exception as e:
        print(f"Error during conversion: {str(e)}")

except Exception as e:

```



```

        print(f"Error in stop_recording: {str(e)}")

def signal_handler(sig, frame):
    print("[INFO] You pressed Ctrl+C! Cleaning up...")
    fps.stop()
    print("[INFO] elapsed time: {:.2f}".format(fps.elapsed()))
    print("[INFO] approx. FPS: {:.2f}".format(fps.fps()))
    cv2.destroyAllWindows()
    vs.stop()
    wiringpi.digitalWrite(FACE_LED_PIN, 0)
    wiringpi.digitalWrite(DOOR_LED_PIN, 0)
    wiringpi.digitalWrite(RELAY_PIN, 1)
    sys.exit(0)

# Load face encodings
print("[INFO] loading encodings + face detector...")
data = pickle.loads(open(encodingsP, "rb").read())

# Initialize video stream
print("[INFO] starting video stream...")
vs = VideoStream(src=1, framerate=5).start()
time.sleep(2.0)

# Start FPS counter
fps = FPS().start()

# Register signal handler
signal.signal(signal.SIGINT, signal_handler)

```

```
# Recording state variables

recording = False

out = None

current_filename = None

recording_start_time = 0

last_motion_time = 0

try:
    while True:
        # Get frame
        frame = vs.read()

        if frame is None:
            continue

        frame = imutils.resize(frame, width=500)

        # Check PIR sensor
        motion_detected = wiringpi.digitalRead(PIR_PIN)
        current_time = time.time()

        # Handle motion recording
        if motion_detected:
            print("Motion detected!")

            if not recording:
                out, current_filename = start_recording()

                if out is not None:
                    recording = True

                    recording_start_time = current_time

                    last_motion_time = current_time
            else:
```

```

last_motion_time = current_time

if out is not None and out.isOpened():
    try:
        resized_frame = cv2.resize(frame, (FRAME_WIDTH, FRAME_HEIGHT))
        out.write(resized_frame)
    except Exception as e:
        print(f"Error writing frame: {str(e)}")
        stop_recording(out, current_filename)
        recording = False
        out = None
        current_filename = None
elif recording:
    # Calculate times
    total_recording_time = current_time - recording_start_time
    time_since_last_motion = current_time - last_motion_time

    # Determine if we should stop recording
    should_stop = False

    # Stop if we've exceeded maximum duration
    if total_recording_time >= RECORDING_DURATION:
        print(f"Stopping recording: reached maximum duration of {RECORDING_DURATION}s")
        should_stop = True

    # Stop if minimum time has passed and no motion for MOTION_RESET_TIME
    elif total_recording_time >= MIN_RECORDING_TIME and time_since_last_motion >=
MOTION_RESET_TIME:
        print(f"Stopping recording: no motion for {MOTION_RESET_TIME}s")
        should_stop = True

```

```

if should_stop:
    stop_recording(out, current_filename)

    recording = False

    out = None

    current_filename = None

elif out is not None and out.isOpened():
    try:
        resized_frame = cv2.resize(frame, (FRAME_WIDTH, FRAME_HEIGHT))

        out.write(resized_frame)

    except Exception as e:
        print(f"Error writing frame: {str(e)}")

        stop_recording(out, current_filename)

        recording = False

        out = None

        current_filename = None

# Check door sensor

if wiringpi.digitalRead(DOOR_PIN) == 1:
    print("DOOR OPEN")

    wiringpi.digitalWrite(DOOR_LED_PIN, 1)

else:
    wiringpi.digitalWrite(DOOR_LED_PIN, 0)

# Face recognition

boxes = face_recognition.face_locations(frame)

encodings = face_recognition.face_encodings(frame, boxes)

names = []

```

for encoding in encodings:

```
matches = face_recognition.compare_faces(data["encodings"], encoding)
```

```
name = "Unknown"
```

if True in matches:

```
matchedIdxs = [i for (i, b) in enumerate(matches) if b]
```

```
counts = {}
```

for i in matchedIdxs:

```
name = data["names"][i]
```

```
counts[name] = counts.get(name, 0) + 1
```

```
name = max(counts, key=counts.get)
```

if currentname != name:

```
currentname = name
```

```
print(f"Face detected: {currentname}")
```

```
wiringpi.digitalWrite(FACE_LED_PIN, 1)
```

```
wiringpi.digitalWrite(RELAY_PIN, 0)
```

```
print("Door is opened")
```

```
time.sleep(3)
```

```
wiringpi.digitalWrite(FACE_LED_PIN, 0)
```

```
wiringpi.digitalWrite(RELAY_PIN, 1)
```

```
print("Door is closed")
```

```
currentname = "unknown"
```

```

names.append(name)

# Draw face boxes
for ((top, right, bottom, left), name) in zip(boxes, names):
    cv2.rectangle(frame, (left, top), (right, bottom), (0, 255, 225), 2)
    y = top - 15 if top - 15 > 15 else top + 15
    cv2.putText(frame, name, (left, y), cv2.FONT_HERSHEY_SIMPLEX, .8, (0, 255, 255), 2)

# Display frame
cv2.imshow("Facial Recognition is Running", frame)
key = cv2.waitKey(1) & 0xFF

if key == ord("q"):
    break

fps.update()

except KeyboardInterrupt:
    if recording:
        stop_recording(out, current_filename)
    signal_handler(None, None)

except Exception as e:
    print(f"An error occurred: {str(e)}")
    if recording:
        stop_recording(out, current_filename)

finally:

```

```
fps.stop()

print("[INFO] elapsed time: {:.2f}".format(fps.elapsed()))

print("[INFO] approx. FPS: {:.2f}".format(fps.fps()))

if recording:
    stop_recording(out, current_filename)

cv2.destroyAllWindows()

vs.stop()

wiringpi.digitalWrite(FACE_LED_PIN, 0)

wiringpi.digitalWrite(DOOR_LED_PIN, 0)

wiringpi.digitalWrite(RELAY_PIN, 1)
```

Web server code

```
from flask import Flask, render_template, send_from_directory, jsonify, request, Response
```

```
import os
```

```
from datetime import datetime
```

```
import mimetypes
```

```
import time
```

```
import sys
```

```
import logging
```

```
app = Flask(__name__)
```

```
# Set up logging
```

```
logging.basicConfig(level=logging.DEBUG)
```

```
logger = app.logger
```

```
RECORDINGS_PATH = 'recordings'
```

```
# Add MIME type for MP4
```

```
mimetypes.add_type('video/mp4', '.mp4')
```

```
# Initialize GPIO
```

```
try:
```

```
    import wiringpi
```

```
    wiringpi.wiringPiSetup()
```

```
    RELAY_PIN = 8
```

```
    wiringpi.pinMode(RELAY_PIN, 1)
```

```
    wiringpi.digitalWrite(RELAY_PIN, 1) # Start with door locked
```

```
    GPIO_INITIALIZED = True
```

```
    logger.info("GPIO initialized successfully")
```


except Exception as e:

GPIO_INITIALIZED = False

logger.error(f"Failed to initialize GPIO: {str(e)}")

@app.route('/')

def index():

return render_template('index.html')

@app.route('/get_videos')

def get_videos():

videos = []

for filename in os.listdir(RECORDINGS_PATH):

if filename.endswith(('.mp4', '.avi')): # Support both formats during transition

file_path = os.path.join(RECORDINGS_PATH, filename)

file_stats = os.stat(file_path)

video_info = {

'filename': filename,

'size': f"{file_stats.st_size / (1024*1024):.2f} MB",

'date': datetime.fromtimestamp(file_stats.st_mtime).strftime('%Y-%m-%d %H:%M:%S')

}

videos.append(video_info)

return jsonify(sorted(videos, key=lambda x: x['date'], reverse=True))

@app.route('/video/<path:filename>')

def serve_video(filename):

def generate():

with open(os.path.join(RECORDINGS_PATH, filename), 'rb') as f:

data = f.read(1024*1024) # Read 1MB at a time

while data:

```

        yield data

        data = f.read(1024*1024)

    if filename.endswith('.mp4'):
        return Response(generate(), mimetype='video/mp4')
    elif filename.endswith('.avi'):
        return Response(generate(), mimetype='video/x-msvideo')

@app.route('/delete_video/<path:filename>', methods=['DELETE'])
def delete_video(filename):
    try:
        file_path = os.path.join(RECORDINGS_PATH, filename)
        if os.path.exists(file_path):
            os.remove(file_path)
            return jsonify({'success': True, 'message': 'Video deleted successfully'})
        return jsonify({'success': False, 'message': 'File not found'}), 404
    except Exception as e:
        return jsonify({'success': False, 'message': str(e)}), 500

@app.route('/control_door', methods=['POST'])
def control_door():
    if not GPIO_INITIALIZED:
        error_msg = "GPIO is not properly initialized"
        logger.error(error_msg)
        return jsonify({'success': False, 'message': error_msg}), 500

    try:
        logger.info("Attempting to open door...")
        # Open door

```

```

wiringpi.digitalWrite(RELAY_PIN, 0)

logger.info("Door opened")


# Wait 3 seconds

time.sleep(3)


# Close door

wiringpi.digitalWrite(RELAY_PIN, 1)

logger.info("Door closed")


return jsonify({'success': True, 'message': 'Door operated successfully'})
except Exception as e:
    error_msg = f"Error operating door: {str(e)}"
    logger.error(error_msg)
    # Make sure door is closed in case of error
    try:
        wiringpi.digitalWrite(RELAY_PIN, 1)
        logger.info("Door closed after error")
    except:
        logger.error("Failed to close door after error")
    return jsonify({'success': False, 'message': error_msg}), 500


def cleanup():
    """Cleanup function to ensure door is locked when server shuts down"""
    if GPIO_INITIALIZED:
        try:
            wiringpi.digitalWrite(RELAY_PIN, 1)
            logger.info("Cleanup: Ensuring door is locked")
        except Exception as e:

```

```
logger.error(f"Cleanup error: {str(e)}")
```

```
import atexit
```

```
atexit.register(cleanup)
```

```
if __name__ == '__main__':
```

```
    # Check if running with sudo
```

```
    if os.geteuid() != 0:
```

```
        logger.warning("This script might need to be run with sudo to access GPIO pins")
```

```
    try:
```

```
        app.run(host='0.0.0.0', port=8080, debug=True)
```

```
    except Exception as e:
```

```
        logger.error(f"Server error: {str(e)}")
```

```
    finally:
```

```
        cleanup()
```