Peoples Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mohamed Khider University of Biskra
Faculty of Exact Sciences
Department of Computer Science

Order N: Start_Up_RTIC_01/M2/2025

Thesis

Submitted in Partial Execution of the Requirements of the Degree of
Master in "Computer Science"
Option: Information and Communication Technology Networks **(RTIC)**

Smart Facial Recognition Security System for Door Access

By:

Sahli Abd Raouf

Hamed Oumaima

Graduating on 4/06/2025 in front of the following committee of juries:

Dr.	Nouer El Houda Zerarka	MCA	President
Dr.	Aloui Imane	MCA	Supervisor
Dr.	Tibermacine Ahmed	MCB	Co Supervisor
Dr.	Roufaida Bettira	MCA	Examiner 1
Dr.	Mohamed Djellab	MCA	Examiner 2

Année Universitaire : 2024 – 2025

[


بسم الله الرحمن الرحيم

Acknowledgements

With a heart full of gratitude, I begin by acknowledging Allah, the Most Gracious, the Most Merciful. Its His blessings, unwavering support, and guidance that have carried me through this entire journey.

My deepest appreciation extends to my esteemed supervisors, Dr. Imane Aloui, and Pr. Ahmed Tebarmacine. Their exceptional mentorship has been instrumental in shaping this thesis. Their invaluable insights, unwavering belief in my abilities, and continuous support proved to be invaluable. I am particularly grateful for their expertise and patience.

I am also grateful to the faculty members and staff of the Computer Science Department at University Mohamed Khider Biskra. Their assistance, encouragement, and academic guidance during my studies played a crucial role in shaping my academic and research pursuits.

Finally, to my family and friends, my deepest thanks for your unwavering support, prayers, and motivation. Your belief in my abilities and constant encouragement have been a driving force behind all my academic achievements.

I acknowledge the contributions of all other individuals, colleagues, and peers who have provided assistance, advice, or support during my research journey. Your contributions, big or small, are deeply appreciated.

Dedication

With a heart full of gratitude and emotion, I would like to express my deepest thanks to those who stood by me, believed in me, and helped shape this journey into what it is today.

First and foremost, **Alhamdulillah** all praise and thanks are due to Allah, whose mercy, guidance, and blessings have carried me through this journey. Without His help, nothing would have been possible.

To my parents

Are the beating heart behind every success I achieve. Your sacrifices, silent prayers, sleepless nights, and unconditional love have carried me through every challenge.I owe you more than words can express.Thank you for believing in me even when I didnt believe in myself.

My dearest mother, Your strength in sickness is my greatest inspiration. Even as you suffer, you teach me resilience, love, and the meaning of sacrifice. This work is a humble gift to you, with all my heart. May Allah grant you healing, peace, and a long life.

My father

To my beloved father, Your silent sacrifices and unwavering support light my path. Thank you for believing in me, always.

To my sisters

Tasnim and Maissone You are my closest companions and my forever friends. Your love, laughter, and encouragement gave me strength during the toughest days. sister Tasnim I wish her success in her baccalaureate exam and to achieve her dreams. My sister Maysoun, I wish her success in her university career.Thank you for always being my safe haven.

To my little brothers,

To my brothers **AbdEl chakour** and good luck in the middle school certificate, and to my brother **AbdEl Moez** and good luck to my younger brother **AbdEl Rahman** ,Your innocent smile and endless curiosity bring joy to my life. May you grow with wisdom, courage, and dreams bigger than the stars.

To my partner in this work

This achievement wouldnt have been possible without your dedication and support. You stood beside me with patience, teamwork, and shared vision. Im grateful for every step we took together

To my Pr, Imane Aloui

With sincere respect and admiration, I thank you for your valuable guidance and mentorship. Your belief in me and your thoughtful encouragement have inspired me to push forward and strive for excellence.

To my friend, Razane

Thank you for being the voice of comfort and positivity. Your kind heart, sincere friendship, and constant encouragement meant more to me than you can imagine.

To Sayah

Thank you for being a source of encouragement and support. Your thoughtful gestures and kind presence were always appreciated

To Pr.Ouaar hadjer,Abbas

Your kindness and warm spirit left a beautiful mark on this journey. Thank you for your generous heart and uplifting words .

Abstract

This thesis presents a total research and realization of an access control system for doors using facial recognition that integrates Artificial Intelligence (AI) and Internet of Things (IoT) technologies. The study begins with the definition of the background, motivation, and issues of access control systems today, particularly the need for effective, secure, and intelligent solutions in residential and institutional environments.

There is a thorough review of the background of facial recognition technology, including the history of its development, the basic processes (data acquisition, detection, feature extraction, matching), and the spectrum of methods from conventional handcrafted approaches to cutting-edge deep learning-based architectures. The various modalities of facial recognition2D, 3D, and thermal imaginghave been explained along with their merits and limitations.

The thesis also considers the application of AI, more specifically deep learning and transfer learning, in biometric recognition systems. The thesis also discusses the application of liveness detection through eye-blinking methods (EAR) and anti-spoofing techniques for enhanced security. IoT integration is realized through the use of Raspberry Pi, which also brings forth its application in real-time communication, device management, and system scalability.

The design and implementation chapter introduces a multi-layered system architecture with software and hardware modules, including ultrasonic sensors for validating distances, YOLO-based spoofing detection, and a MySQL database to hold real-time data. A 3D design of the door access system is also modeled to visualize the deployment setting. Performance metrics are utilized in assessing the effectiveness of the system in real-world scenarios.

Key words : Face Recognition , Screen Detection ,blink Detection , MTCNN , Facenet, YOLOv8s , Dlib(EAR) , Transfer Learning , Artificial intelligence , IoT .

Résumé

ce travail présente l'ensemble des recherches et la réalisation d'un système de contrôle d'accès pour portes utilisant la reconnaissance faciale, intégrant les technologies de l'intelligence artificielle (IA) et de l'Internet des objets (IoT). L'étude débute par la définition du contexte, des motivations et des enjeux des systèmes de contrôle d'accès actuels, notamment le besoin de solutions efficaces, sécurisées et intelligentes dans les environnements résidentiels et institutionnels.
Une analyse approfondie du contexte de la technologie de reconnaissance faciale est effectuée, incluant l'historique de son développement, les processus fondamentaux (acquisition de données, détection, extraction de caractéristiques, appariement) et l'éventail des méthodes, depuis les approches artisanales conventionnelles jusqu'aux architectures de pointe basées sur l'apprentissage profond. Les différentes modalités de reconnaissance faciale 2D, 3D et imagerie thermique sont expliquées, ainsi que leurs avantages et leurs limites.
La thèse examine également l'application de l'IA, plus particulièrement l'apprentissage profond et l'apprentissage par transfert, aux systèmes de reconnaissance biométrique. Elle aborde également l'application de la détection du vivant par clignement des yeux (EAR) et des techniques anti-usurpation d'identité pour une sécurité renforcée. L'intégration de l'IoT est réalisée grâce à Raspberry Pi, qui permet également d'optimiser les applications de communication en temps réel, de gestion des appareils et d'évolutivité du système.
Le chapitre ńăConception et mise en uvreăż présente une architecture système multicouche avec des modules logiciels et matériels, notamment des capteurs à ultrasons pour la validation des distances, la détection d'usurpation d'identité basée sur YOLO et une base de données MySQL pour le stockage des données en temps réel. Une conception 3D du système d'accès aux portes est également modélisée afin de visualiser les paramètres de déploiement. Des indicateurs de performance sont utilisés pour évaluer l'efficacité du système en situation réelle.

Mot clés : Reconnaissance faciale, détection d'écran, détection de clignement, MTCNN, Facenet, YOLOv8s, Dlib (EAR), apprentissage par transfert, intelligence artificielle, IoT.

Contents

List of Figures

Chapter 1

General Introduction

1.1 Context

Security remains a fundamental concern in both residential and commercial settings, necessitating reliable and efficient access control systems. Traditional locking mechanisms, such as keys, PIN codes, and RFID cards, present significant vulnerabilities, including key loss, forgotten passwords, theft, or unauthorized duplication [1]. Although password protection at the entrance using RFID between the door and the control panel is cost-effective, it is easily compromised by advanced techniques such as data interception, command decryption, and replay attacks on the control panel [2]. Additionally, these signals can be jammed to prevent alerts by transmitting wireless noise, blocking the signal from reaching the control panel from the sensors [3].

In contrast, biometric authentication methods offer enhanced security and user convenience by leveraging unique physiological characteristics [4]. Among the most commonly used biometric technologies, facial recognition stands out alongside fingerprint recognition [5]. Facial recognition is particularly notable for its non-intrusive nature and high accuracy in identity verification [6]. Unlike many traditional technologies, facial recognition does not require physical contact, keys, or physical cards. The system can detect a human face from an image or video and then compare and analyze predefined facial features stored in a database. Its ease of use makes it an ideal choice for access control systems [7]. However, challenges such as lighting variations, pose changes, and privacy concerns must be addressed to ensure reliability and user acceptance.

This project aims to address these challenges by designing and implementing a face recognition-based smart door lock system using artificial intelligence algorithms and real-time processing. The system enhances security while maintaining a robust event logging and monitoring system for access events.

1.2 Problematic and Motivation

The motivation for this work is the growing need for high-tech security solutions with reliable access control that does not compromise on convenience for the users. Face recognition is a quick and convenient authentication method that removes risks associated with traditional keys and access cards. As a response, the integration of this technology with IoT devices, i.e., Raspberry Pi, transforms smart home and building security, unlocking possibilities for novel and intuitive security solutions. By addressing the current problems and leveraging AI advancements, this project aims to contribute to creating a secure, intelligent, and responsive facial recognition system.

This project aims to resolve these problems by designing and implementing an AI-powered facial recognition door lock system with real-time processing. The system offers enhanced security with a robust logging and monitoring system for door access events.

1.3 Objectives of the Study

The primary objectives of this research are to develop an artificial intelligence-based door access system using facial recognition in order to enhance security. The system will be in a manner such that it is real-time face detection and classification through advanced algorithms, resulting in a secure and effective way of access control. The system will also be connected with a Raspberry Pi to securely control an electric lock, providing physical security within the area. In order to effectively control entry control, the system will have a central server with an exhaustive database of accepted and rejected faces. The server will also have a web-based interface for real-time monitoring, logging, and user management for ease of use. Other than this, to guarantee the integrity and confidentiality of information, secure communication among all the components of the system will be guaranteed by the implementation of TCP/IP protocols.

1.4 Structure of the Thesis

The dissertation comprises four chapters, each addressing a distinct research component. Heres a chapter breakdown:

- **Chapter 1 : Background on Facial Recognition** , covers the definition and history of facial recognition, the main steps of the process, e.g., feature extraction and classification methods. It covers the technologies and algorithms used, e.g., OpenCV and TensorFlow, and system performance-influencing factors, e.g., lighting, pose variation, and resolution. Additionally, the chapter also discusses the applications of facial recognition as a security and access control component, providing its advantages and limitations as a biometric authentication solution.

- **Chapter 2 : State of the Art in Security Methods**, provides a review of traditional as well as modern security systems, categorizing access control techniques as keys, codes, RFID, and biometric systems. It reports work carried out on face recognition as a security technique, providing a comparative analysis of previous systems to identify strengths, weaknesses, and areas of improvement. This chapter sets the foundation of the proposed system by putting its applicability in perspective with evolving security approaches

- **Chapter 3 : Design and implementation**, outlines the complete architecture of the discussed facial recognition-based door access system. It provides detailed design of the hardware modules, including the camera, server, Raspberry Pi, and electric lock, so that all modules are smoothly integrated. The chapter further discusses the communication protocols and data flow required for effective and secure system operations, laying down a foundation for the implementation process.

- **Chapter 4 : Experimentation results and Discussion**,This chapter presents the experimental setup and evaluation of the proposed system. It outlines the methodology used to test the performance and effectiveness of the model, including the datasets, metrics, hardware environment, and testing scenarios. The chapter also discusses the results obtained from various experiments, including model accuracy, reliability, and the systems real-time performance under different conditions. Furthermore, it analyzes challenges encountered during testing and explains how these were addressed to improve the overall robustness of the system.

Chapter 2

Background on Facial Recognition

2.1 Introduction

In recent years, artificial intelligence (AI) [9] has advanced rapidly, enabling the development of transformative technologies such as self-driving cars [10] and automated retail environments. Central to many AI applications is computer vision, a field focused on replicating human visual perception through machines. While human vision effortlessly processes complex environments, replicating this ability electronically requires sophisticated image interpretation capabilities.

Computer vision enables machines not only to perceive images but also to interpret, react, and make decisions based on visual input. This involves complex processes like detection, identification, reasoning, and decision-making, functions that mimic the human visual and cognitive system. However, since most visual sensors capture two-dimensional images while the world exists in three dimensions, interpreting depth and spatial relationships adds complexity to machine vision systems.

Facial recognition, as a subset of computer vision, has emerged as a key application area, revolutionizing security, access control, and user authentication. This chapter introduces facial recognition technology, exploring its historical evolution, operational mechanisms, system types, feature extraction methods, recognition frameworks, and real-world applications[11].

2.2 Historical Background

Automated facial-recognition technology is a relatively new concept. It arose in 1960s, when the first semi automated system for facial recognition was developed. It was based on a method whereby facial features were located by the observer on the photographs of the subject. In the next step, specific to a reference point, distances and ratios were calculated, which then enabled comparisons to be made. The reference point was common for all facial features.

The domain of automated facial-recognition technology was founded by Woody Bledsoe, Helen Chan Wolf, and Charles Bisson. In 19641965, they worked together to recognise human faces using a computer.[12] In the 1970s, 21 subject-specific features, such as lip thickness and hair color, were used for automated facial recognition.[13] The problem with this approach, however, was that the measurements were taken and calculated manually. In 1988, the principal component analysis (PCA) method was applied by Sirvoich and Kirby to try to solve the facial-recognition problem.[14] This was thought to be a turning point in the world of face recognition, as it proved to code and normalise a facial image accurately, and fewer than 100 values were required. In 1991, Turk and Pentland discovered that while implementing Eigenfaces method, the residual error could be used for facial recognition.[15] This discovery enabled the reliability of an automated facial-recognition system, although the approach was restricted by environmental conditions.

In 1997, ZN-Face software was developed and com mercialised. The software worked well enough to rec ognise facial images with occlusions, even including images that were not perfectly frontal. In todays arena, this technology is widely used in image process ing and pattern recognition, and has become an area of active research.

Today, several attempts are also being made to study real-world facial-recognition challenges.[16] Moreover, the impact of side faces on facial recognition has also recently become an active area of research, although the accuracy of this is only 50% to date.[17] However, in one recent study, the importance of one profile of the face was highlighted, showing that the sensitivity and specificity of human identification through this approach has increased significantly.[18]

2.3 Definition Of Face Recognition

Face recognition is part of computer vision. Face recognition [19] is used to identifying a person in biometric method based on image on their face. A person is identified through biological traits. Human eyes can easily recognize people by simply looking at them but the concentration span for human eyes has its limit. Hence, a computerized method is invented to perform face recognition. Face recognition [20] includes the operations of automatically detecting followed by verifying a person from either picture or video. Although face recognition has been researched extensively [21, 22]

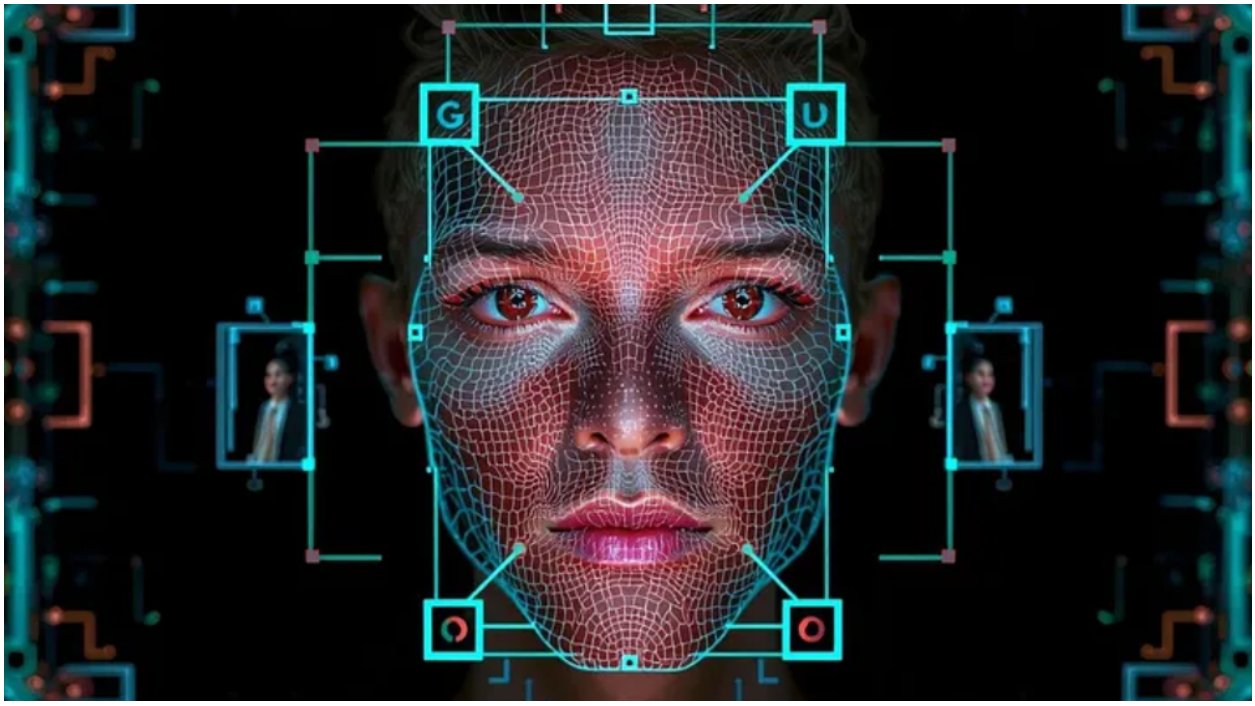

Figure 2.1: Face Detection. [114]

2.4 How Facial Recognition Works

The process of facial recognition involves a series of steps, ranging from data acquisition to the final stage of matching. While the specifics may vary between different types and models of facial recognition systems, the general process remains the same.

2.4.1 Data Acquisition

The first step in facial recognition is data acquisition or the collection of facial data. This is typically done using cameras that capture either 2D images, 3D images, or thermal images, depending on the type of system. images can be taken from various sources such as video surveillance, smartphone cameras, or dedicated facial recognition devices.[23]

2.4.2 Face Detection

Once an image is captured, the next step is to detect the presence of any faces in the image. This process involves identifying and locating human faces in digital images. Advanced algorithms are used to scan the entire image and distinguish facial features from the rest of the image based on certain properties or features such as the structure, color, and shape of the face. [23]

2.4.3 Feature Extraction

After detecting a face in an image, the system then moves on to feature extraction. This process involves identifying and measuring distinct facial features and converting them into numerical data. The facial features that are commonly measured include the distance between the eyes, the width of the nose, the depth of the eye sockets, the shape of the cheekbones, and the length of the jawline, among others. Different facial recognition systems extract and use different types of features. Some systems, like eigenface-based systems, look at the face as a whole and capture holistic features. Others, like local feature analysis systems, focus on specific local features like the eyes, nose, and mouth[23]

2.4.4 Matching

The final step in the facial recognition process is matching. This involves comparing the extracted features with the stored facial data in the database. In identification mode, the system compares the features with all the facial data in the database to find a match. In verification mode, the system compares the features with the stored data of a specific individual to confirm their identity.

In some systems, the match is determined based on a similarity score. If the similarity score crosses a certain threshold, the system concludes that it has found a match.

In recent years, machine learning, and more specifically deep learning, has been widely used in feature extraction and matching processes. Deep learning algorithms can learn to recognize patterns in the facial data, improving the accuracy and efficiency of the facial recognition process.

In summary, the overall process of facial recognition technology is shown in Figure 2.1, facial recognition involves a combination of sophisticated techniques and technologies. While the steps of data acquisition, face detection, feature extraction, and matching form the basis of all facial recognition systems, the specific implementation of each of these steps can vary widely, leading to different levels of performance and accuracy.[23]

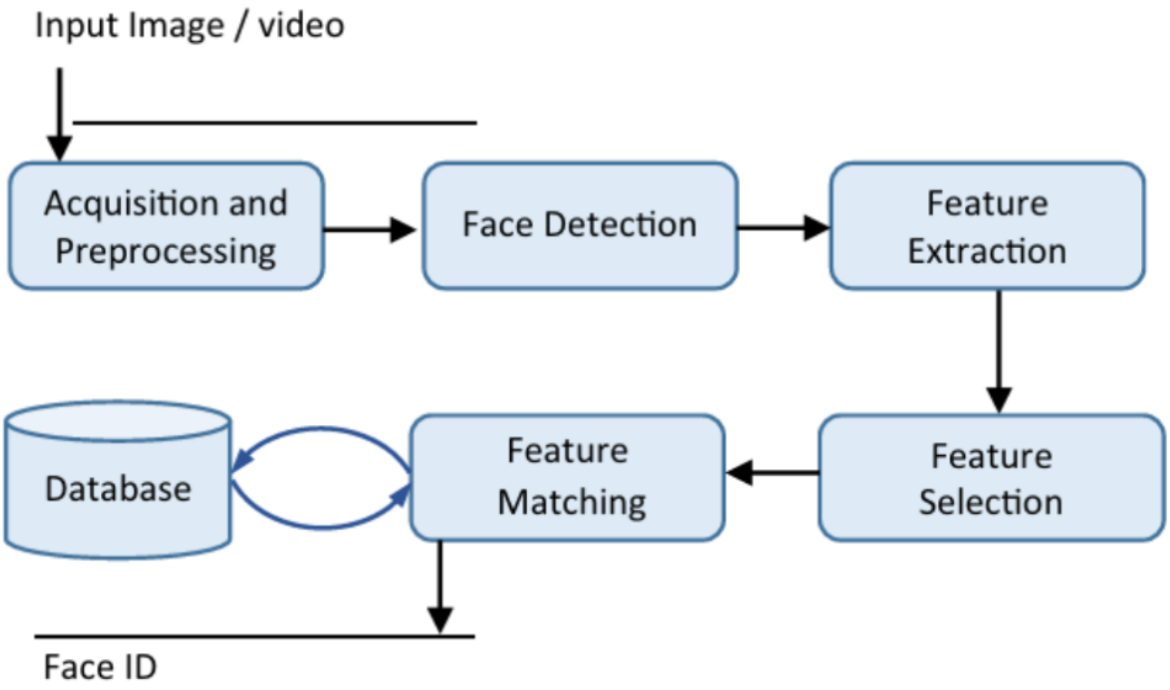

Figure 2.2: An overview of Face Recognition system [52]

2.5 Types of Facial Recognition Systems

Facial recognition technology has evolved significantly over the years, leading to the development of multiple systems with different techniques for capturing and analyzing facial data. Broadly, these systems can be classified into three categories: 2D Facial Recognition, 3D Facial Recognition, and Thermal Facial Recognition.

2.5.1 2D Facial Recognition :

2D facial recognition is the most common and widely used form of facial recognition technology[24]. It operates by capturing a two-dimensional image of a persons face and then comparing or verifying this image with stored 2D facial data. The most crucial factor in this type of system's success is the lighting conditions during the capture of the facial image. Changes in lighting can lead to changes in the appearance of facial features, which can potentially reduce accuracy.

2D facial recognition systems are also sensitive to the angle of the face[25]. They work best when the face is directly facing the camera, and performance tends to decrease when the face is turned to the side or tilted up or down. To mitigate this, advanced 2D facial recognition systems use AI techniques to estimate the appearance of the face from different angles.

Despite these challenges, 2D facial recognition systems have been widely adopted due to their relative simplicity and lower cost compared to other types. They are used extensively in various applications, including smartphone unlocking, photo tagging on social media, and security surveillance.

2.5.2 3D Facial Recognition :

3D facial recognition systems add another dimension to the process, capturing a three-dimensional model of a face. This technology maps the face's unique features such as the curves of the eye socket, nose, and chin which remain unaffected by lighting conditions or facial expressions[26].

3D facial recognition technology uses depth sensors or stereo cameras to capture the precise shape and contours of a face. The collected data is then used to identify or verify a person's identity. Since these systems use 3D data, they are less affected by changes in lighting or face angle[27], making them more accurate in various conditions compared to 2D systems.

However, 3D facial recognition systems are generally more complex and costly to implement. They also require more processing power to analyze the 3D facial data. Despite these challenges, they are becoming increasingly popular, particularly in high-security applications where a high level of accuracy is required.

2.5.3 Thermal Facial Recognition :

Thermal facial recognition is a relatively new and less common type of facial recognition technology. It uses thermal cameras to capture the heat patterns that are emitted from the face[28]. These heat patterns, which are unique to each individual, can be detected in both light and dark environments, making this system highly effective regardless of lighting conditions.

Thermal facial recognition has shown potential in various applications, especially those that require the detection of faces in poorly lit or nighttime conditions[29]. However, the technology is still in its early stages of development, and the cost of thermal cameras can be a limiting factor for widespread adoption.

In conclusion, each type of facial recognition system has its strengths and weaknesses, and the choice of system depends on the specific requirements of the application. The advancement of technology and research is likely to lead to improvements in these systems and possibly the development of new types that leverage other facial characteristics or technologies. The future of facial recognition technology is exciting, with boundless possibilities for innovation and application.

2.6 Feature extraction techniques:

For any face recognition system to be successful, feature extraction is essential. It involves turning unprocessed facial images into useful numerical representations, also referred to as features or embeddings, that capture the key characteristics of an individual's face. Individuals are then accurately and efficiently compared and recognized using these features. **Three major groups can be used to broadly classify feature extraction techniques:**

2.6.1 Handcrafted Feature-Based Methods

These traditional methods extract facial patterns,like texture or edge orientation, using preset algorithms. Principal Component Analysis (PCA), Histogram of Oriented Gradients (HOG) are a few examples. They are easy to implement and require little computing power.For example:
PCA is a technique that takes high-dimensional image data and uses the dependencies between the variables to represent it in a more tractable, lower-dimensional form without losing too much information.PCA is a statistical procedure that evaluates the covariance structure of a set of variables and identifies the principal directions in data variables. PCA is used to identify sets of orthogonal coordinate axes through the data. Principal components are determined by computing the eigenvectors and eigenvalues of the data covariance matrix. Based on principal components, the identification of face images is performed.[30]

2.6.2 Fast Matching-Based Methods

These techniques focus on extracting lightweight binary features optimized for rapid matching, often used in resource-constrained environments. Methods such as Four-Patch Binary Pattern Matching (FPBM), BRIEF, and ORB enable real-time face comparisons with minimal computational overhead.Ex:
FPBM is a method to extract the features of the images on the basis of matching image areas and subpixel displacement estimates using similarity measures.The recognition is based on the edge detection. This method generates much less information than the original image has. This is because it eliminates most of the details that are not relevant for the purpose of identifying the boundaries, while preserving the essential information to describe the shape and structural characteristics and geometry of the objects represented.[30]

2.6.3 Deep Learning-Based Methods

Convolutional neural networks (CNNs) are used in these contemporary methods to automatically extract rich, discriminative facial features from sizable datasets. State-of-the-art performance in face recognition tasks is provided by models like FaceNet, VGGFace, and ArcFace, which generate compact embeddings that capture high-level facial characteristics.For example:

CNN deep learning model are used to study the unconstrained facial expression. The general process of feature extraction is as follows:

- Modify the face image by eye location algorithm, reduce the test sample and training sample to $90x150$ pixels by bilinear interpolation method, and perform the preprocessing process of histogram equation and other data.
- Use 40 Gabor filters (using 40 directions and different scales) to refine the preview image to obtain all samples.
- Using **LQP** operator, Gabor image and test sample are divided into $9x15 = 135$ small rectangular blocks, and each LQP operator is used to separate the texture of each sub block and connect each sub function. Concatenate the features of each sub block to establish a sample GLQP attribute.
- **GLQP** was used to characterize the training samples according to CNN. It is used as input and iterates 500 times.
- **CNN** is used to optimize the contour features of experimental samples, and the fusion features of local features and global features are used as partition input to classify and recognize facial images,and the results are counted to establish a complete face recognition system.[31]

Each category brings unique advantages depending on the application, whether it's accuracy, speed, or resource efficiency. The choice of technique depends on system requirements such as hardware limitations, recognition accuracy, and processing time.While traditional methods are fast and simple, deep learning models offer greater accuracy and robustness by learning complex patterns directly from large datasets.

2.7 Face recognition frameworks

Since, face recognition has been a key research area for the last three decades by many research communities like machine learning, artificial intelligence, image processing, and computer vision. Methods proposed for face recognition belong to vast and diverse sci entific domains and that is why it is difficult to draw a clear line that categorizes these approaches in a standard way. Also, the usage of hybrid models makes it difficult to cat egorize these approaches in standard branches for feature representation or classification. However, according to recent literature, we sum-up and present face recognition approaches as a clear and high-level categorization. Figure 2.3 shows the categorical distribution of face recognition approaches:

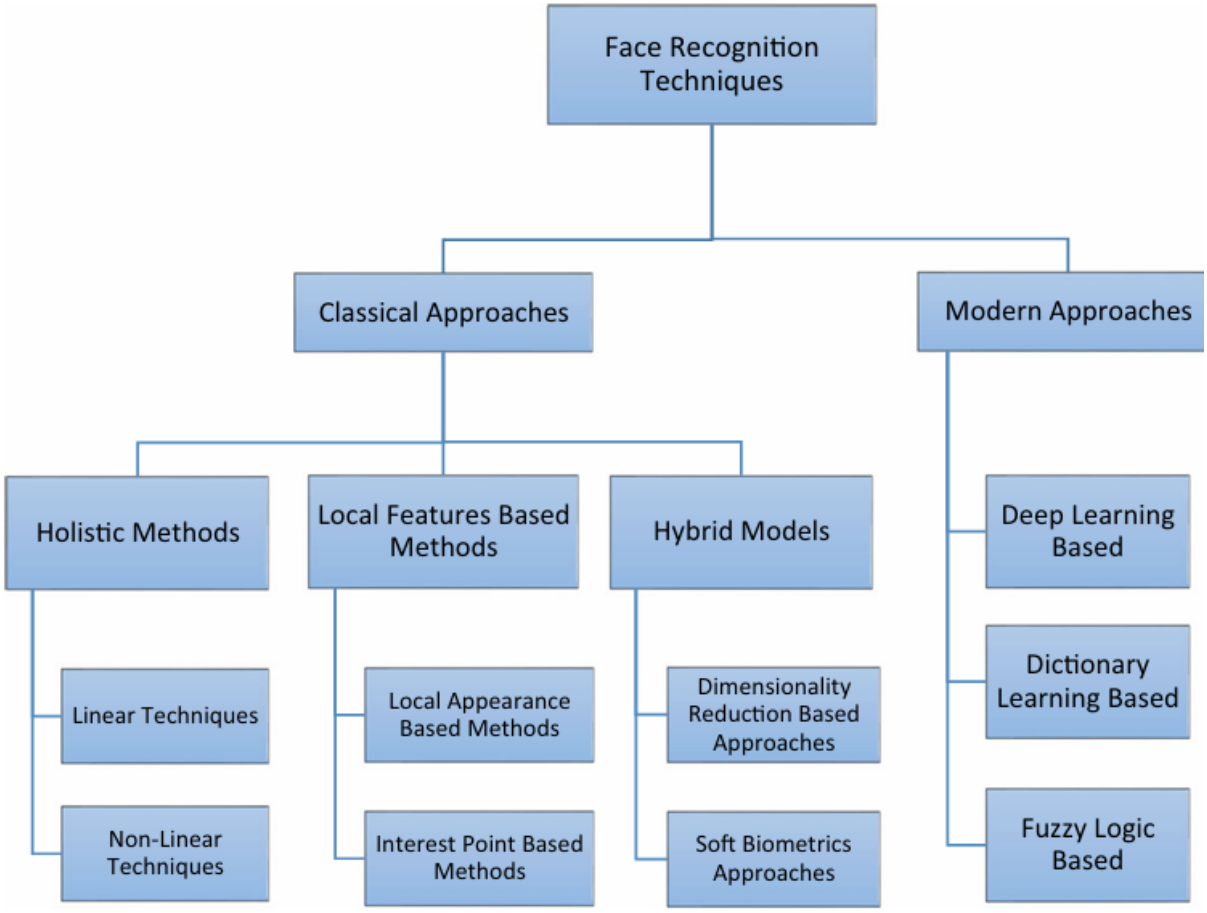

Figure 2.3: Categorical distribution of face recognition methodologies[52]

2.7.1 Classical approaches

The research in face recognition has long historic roots such as in the 1950s psychology and 1960s in engineering literature [32]. These beginning concepts were derived from pattern recognition systems as discussed in an MIT Ph.D. thesis [33] by Lawrence Gilman. He first identified that a 2D features extracted from a photograph can be matched with the 3-D representation. Subsequent research identified practical difficulties in variable environmen tal conditions which are still challenging with todays modern supercomputers and GPUs. Although these early research methods have been driven by pattern recognition, they were based on the geometrical relationships between facial points. Most of these methods are obviously highly dependent on detection of these facial points in a challenging environment as well as the consistency of these relationships across different variations. These issues are still a critical challenge for the research community. Another early attempt for developing face recognition system was by Kanade et al. [34]. They utilize simple image processing techniques to extract a vector of 16 facial parameters. It used a simple Euclidean distance measure for matching these feature vectors and achieve 75% accuracy rate on a predefined database of 20 people using 2 images per person.

In 2003, Zhao et al. [32] presented a precise and brief overview of techniques being employed by face detection and recognition community during last 30 years. They discuss many psychological and neuroscience aspects of face recognition. As for the method is concerns, face recognition techniques are initially categorized into three broad ways, holis tic methods (PCA, LDA, SVM, ICA, FLD and PDBNN), features based methods (pure geometry methods, dynamic link architecture, Hidden Markov Model and Convolution Neural Network) and many hybrid methods like Modular Eigenfaces, Hybrid LFA, Shape normalized and component based methods

2.7.2 Modernapproaches

In recent years, there is an immense improvement due to machine learning-based algorithms and methodologies in a lot of social and scientific domains. We summarize the modern era of face recognition approaches as three subcategories i.e. deep learning-based methods, sparse or dictionary learning-based methods and fuzzy logic-based techniques. An overview and research contributions in these categories are presented in this section.

2.7.2.1 Deeplearning basedfacerecognition

It has been observed that deep neural networks have massive computational power for object recognition and it has revolutionized machine learning during the last few years. Researchers from all the fields including but not limited to social sciences and engineer ing to life sciences considering deep frameworks to hybridize their existing models and get radical results. Many researchers, especially in face recognition community [35, 36], affirms that it has remarkable computational power with outstanding accuracy and result oriented behavior. In this section, we present a brief overview of recent developments in deep learning for face recognition.

2.7.2.2 Dictionary Learning for Face Recognition:

Dictionary learning is a branch of machine learning algorithms that aims to find a matrix called dictionary in which a training data CNN stands for Convolutional Neural Network, DCNN represents Deeper Convolutional Neural Network, and DCGANrefers to Deep Convolutional Generative Adversarial Network submits a sparse representation. In our context, if collections of face samples are there in a random distribution, we can extract discriminative features by learning the desired dictionary from training data. The learned dictionary plays a vital role in the success of the sparse representation [37]. We have to learn a task-specific dictionary from the given face images. Therefore, as an emerging research field, existing theories and approaches for feature representation need to be rebuilt for dictionary learning.

2.7.2.3 Fuzzy set theory

Primarily, the fuzzy set theory was introduced in 1965 by Lotfi Aliasker Zadeh [38]. Since its inception, it has been applied in a variety of disciplines such as logic, decision the ory, operations research, computer science, artificial intelligence, pattern recognition, and robotics, etc. Especially, during the last few years, its adoption has revolutionary changed the various research domains. The power of fuzzy set theory for face recognition in light of recent developments. It has been noticed that fuzzy-based methods are highly potential for dealing with complex face recognition issues, especially illumination and pose variation related complexities.

2.8 Factors Influencing Recognition Accuracy :

Since it was developed, the area of facial recognition has often had to overcome obstacles, there being several factors which make precise recognition a challenging task, as outlined below:

- **Illumination**: Variable lightning conditions can have a number of different effects on a persons facial image.[39]
- **Pose**: The problem of pose has been identified as a key issue in face recognition, and it has been the subject of much interest amongst the research community in recent decades.[40]
- **Occlusion**: Amongst many issues associated with accurate facial recognition, handling facial occlusion is one of the major issues.[41] When any portion of the face is occluded, facial features cannot be fully viewed, and therefore, authentication by the facial recognition system is at risk.
- **Expressions**: Human faces always contain expres sions of one sort or another, these being generally underpinned by the emotional state of the individu al. Face-recognition systems are also affected by human expressions, which result from the movement of the facial muscles, leading to changes in facial images.[42]

  However, some face-recognition systems are unable to process different expressions by the same person, meaning that a problem can arise with identification.[43]
- **Hair** : Hair often covers the forehead. Hence, in most face-recognition systems, database images have hair neutralised in order to prevent it from acting as a barrier to the recognition of faces. Research is being undertaken to try to solve this problem.[44]
- **Age**: With the progression of age, the facial features can change tremendously. This area of research is, however, still at an early stage, and much more needs to be done.[4]

2.9 Applications of Facial Recognition Technology:

Facial recognition technology has seen a surge in applications across a wide range of industries, driven by its potential to enhance security, convenience, and personalization.

Figure 2.4: Uses of Face Detection[115]

- **Security and Surveillance** One of the most significant applications of facial recognition technology is in security and surveillance. Law enforcement agencies across the globe use facial recognition to identify individuals in surveillance footage[45], helping to solve crimes and enhance public safety. The technology is also widely used in access control systems, providing secure entry to buildings or rooms by verifying the identity of individuals[46].

- **Smartphone Authentication** Various phones, including the most recent iPhones, use face recognition to unlock the device. The technology offers a powerful way to protect personal data and ensures that sensitive data remains inaccessible if the phone is stolen. Apple claims that the chance of a random face unlocking your phone is about one in 1 million.[91]

- **Social Media** Social media platforms like Facebook use facial recognition technology to automate the tagging of individuals in photos. By recognizing and remembering the facial data of users, these platforms can suggest tags for people in newly uploaded photos, enhancing the user experience and connectivity among users[47].

- **Healthcare** Hospitals use facial recognition to help with patient care. Healthcare providers are testing the use of facial recognition to access patient records, streamline patient registration, detect emotion and pain in patients, and even help to identify specific genetic diseases. AiCure has developed an app that uses facial recognition to ensure that people take their medication as prescribed. As biometric technology becomes less expensive, adoption within the healthcare sector is expected to increase.

- **Education and Workforce** Some educational institutions in China use face recognition to ensure students are not skipping class. Tablets are used to scan students' faces and match them to photos in a database to validate their identities. More broadly, the technology can be used for workers to sign in and out of their workplaces, so that employers can track attendance.[91]

- **Automotive** According to this consumer report, car companies are experimenting with facial recognition to replace car keys. The technology would replace the key to access and start the car and remember drivers preferences for seat and mirror positions and radio station presets.[91]

- **Airports** Facial recognition has become a familiar sight at many airports around the world. As well as at airports and border crossings, the technology is used to enhance security at large-scale events such as the Olympics.[91]

These applications represent just a fraction of the potential uses of facial recognition technology. As the technology continues to advance, it is likely to be integrated into even more areas, including banking, travel, entertainment, and more. Despite the impressive benefits and applications, facial recognition technology also presents notable challenges, including accuracy concerns and issues related to privacy and ethics, which need to be carefully managed as the technology continues to evolve.

2.10 Advantages of face recognition

- **Increased security** On a governmental level, facial recognition can help to identify terrorists or other criminals. On a personal level, facial recognition can be used as a security tool for locking personal devices and for personal surveillance cameras.[91]

- **Crime Reduction** Face recognition makes it easier to track down burglars, thieves, and trespassers. The sole knowledge of the presence of a face recognition system can serve as a deterrence, especially to petty crime. Aside from physical security, there are benefits to cybersecurity as well. Companies can use face recognition technology as a substitute for passwords to access computers. In theory, the technology cannot be hacked as there is nothing to steal or change, as is the case with a password.48

- **Removing bias from stop and search** Public concern over unjustified stops and searches is a source of controversy for the police facial recognition technology could improve the process. By singling out suspects among crowds through an automated rather than human process, face recognition technology could help reduce potential bias and decrease stops and searches on law-abiding citizens.[91]

- **Greater convenience** As the technology becomes more widespread, customers will be able to pay in stores using their face, rather than pulling out their credit cards or cash. This could save time in checkout lines. Since there is no contact required for facial recognition as there is with fingerprinting or other security measures useful in the post-COVID world facial recognition offers a quick, automatic, and seamless verification experience.[91]

- **Faster processing** The process of recognizing a face takes only a second, which has benefits for the companies that use facial recognition. In an era of cyber-attacks and advanced hacking tools, companies need both secure and fast technologies. Facial recognition enables quick and efficient verification of a persons identity.[91]

- **Integration with other technologies** Most facial recognition solutions are compatible with most security software. In fact, it is easily integrated. This limits the amount of additional investment required to implement it[91].

2.11 Challenges of Facial Recognition Technology:

Despite its impressive capabilities and growing applications, facial recognition technology is not without its challenges and limitations.

2.11.1 Accuracy and Biases

Although facial recognition technology has significantly improved over time, there are still concerns about its accuracy. Changes in lighting, facial expressions, aging, and the use of accessories like glasses or hats can sometimes affect the performance of facial recognition systems. Additionally, some facial recognition systems have been criticized for racial and gender biases[48], with lower accuracy rates observed for certain demographic groups. This has raised serious concerns about the fairness and reliability of the technology.

2.11.2 Privacy Concerns

The widespread use of facial recognition technology has also raised substantial privacy concerns[49]. The ability to identify and track individuals in public spaces could potentially lead to mass surveillance, infringing on people's privacy rights. There are also concerns about the storage and handling of sensitive facial data[50], which, if not properly protected, could be vulnerable to data breaches or misuse

2.11.3 Dependence on Quality of Input Data

The performance of facial recognition systems heavily depends on the quality of the input data. Low resolution images or images captured at odd angles can lead to inaccurate results. This dependence on input quality can limit the effectiveness of facial recognition in certain scenarios[**?**]. Despite these challenges and limitations, the potential of facial recognition technology is immense. As the technology continues to evolve, it is likely that solutions to these challenges will be developed. Ongoing research and development, coupled with thoughtful regulation and ethical considerations, can help to ensure that the benefits of facial recognition technology are realized while minimizing potential drawbacks.

2.12 Conclusion

This chapter has provided a comprehensive overview of facial recognition technology,beginning with its historical development and progressing through its operational mechanisms, technical foundations, and key application areas. We explored how facial recognition evolved from early manual and statistical techniques to todays sophisticated deep learning-based systems capable of real-time identification in dynamic environments.

A detailed discussion was presented on how facial recognition systems operate, from data acquisition and face detection to feature extraction and matching. We classified different types of facial recognition systems (2D, 3D, thermal), described key feature extraction methods (handcrafted, fast matching, deep learning), and outlined both classical and modern recognition frameworks. Additionally, we examined the various factors influencing recognition accuracy, such as lighting, pose, occlusion, and aging.

The chapter also emphasized the increasing importance of facial recognition across a broad range of applications, from law enforcement and access control to healthcare, education, and consumer electronics. Furthermore, we highlighted how integration with emerging technologies such as IoT, cloud computing, blockchain, and edge AI expands the reach and functionality of facial recognition systems.

While the advantages of facial recognition are considerable, enhancing security, convenience, and operational efficiency, the technology is not without its challenges. Issues such as privacy concerns, bias, data dependency, and the risk of misuse underscore the importance of ethical design and regulatory oversight.

Facial recognition stands as a powerful and rapidly evolving field within AI and computer vision. Understanding its foundational concepts and current capabilities sets the stage for a deeper exploration of its application in security technologies, which is the focus of the next chapter.

Chapter 3

State of the art on facial recognition methods as a security technology

3.1 Introduction

Over the past few decades, security technologies have undergone a major transformation, evolving in response to the increasing complexity of modern threats. What previously relied largely on mechanical deterrence and manual verification has now transformed into intelligent and predictive systems capable of real-time monitoring, threat assessment, and autonomous response. Todays security infrastructures integrate a variety of technologies, including closed-circuit television (CCTV) cameras, intrusion detection systems, biometric authentication, and artificial intelligence (AI)-based analytics, to create multi-layered structures that protect people, property, and critical infrastructure [53], [54]. Among these technological developments, biometric-based systems, including facial recognition, have emerged as a pioneering innovation in the field of access control.

For high-security environments, such as airports, government buildings, and corporate campuses, these systems offer fast, contactless and accurate identification capabilities. Traditional credentials such as keys or access cards, which are particularly vulnerable to loss, theft, and duplication, are replaced by facial recognition systems [55]. Therefore, the technological development and strategic need to increase operational security, public safety and the effectiveness of modern security systems is to integrate AI-enhanced biometric technologies into access control systems [56].

To understand the evolution of these systems, it is necessary to understand the history of the development of door locking systems, which led to the emergence of modern intelligent systems. The following section traces the evolution of lock technology to illustrate how centuries of mechanical development paved the way for the digital and biometric access control systems we know and take for granted today.

3.2 History and evolution of locking door systems

The use of locking systems goes back over six thousand years ago, to ancient Egypt; where people developed the first wooden pin tumbler locks. These initial systems were simple;consisting of a wooden pin tumbler mechanism using wooden pins, operated by a large wooden key that resembled a contemporary toothbrush[57]. This method was primitive, but the foundation for secure access and entry control mechanisms.[59]

Locking mechanism technology developed considerably during the Roman era. For example, different metals such as bronze, silver, and even gold were used to create more secure and complex locks than their predecessors. During this time, padlocks were displayed to the public as a sign of high social status. Some wealthy people even gave expensive keys as jewelry [7]. The Industrial Revolution of the 19th century brought sudden mass production and the use of more durable materials such as steel and copper, resulting in increased security and a more reasonable price than before this period. Initially, lock technology relied on the end user's ability to circumvent it, but technological advances, such as the invention of the pin tumbler lock, not only increased security but also led to the development of more intrusion-resistant locks. Although cylinder locks are still widely used today, new technologies, including electronic locking devices and biometric locks, have redefined security [60].

By the 20th century, the locksmith profession was no longer considered a craft, but rather a profession where the locksmith specialized in the technical aspects of maintaining and repairing locks, as well as unlocking them. Mechanical locks became widespread in residential, commercial, and institutional settings. Many variations of mechanical locks emerged over the years; deadbolts, padlocks, and combination locks all addressed different security challenges. While reliable, mechanical locks could still be forced, keys could still be duplicated, and locks could wear out over time [61]

The integration of information technology and security challenges in the 21st century has led to the development of electronic and intelligent locking systems. These systems include not only keypad locking systems and remote controls, but also RFID-based locking systems and, more recently, biometric systems using fingerprint, iris, and facial scanning technologies. Electronic and intelligent locking systems offer more features, such as remote access control, usage logging, and connection to other security systems [62], but they also introduce new vulnerabilities, such as software failures and cyber threats [63].

Despite many challenges, door-locking technologies have evolved from mechanical to intelligent in a linear, even predictable, manner. The latest systems, which leverage artificial intelligence and biometrics, are just the latest step in a long journey toward protecting physical space. However, they demonstrate that the fundamental aspects of a door lock have not changed: security and access control, now much more efficient and intelligent [64].

3.3 Classification of access security methods

When considering the historical evolution of locking mechanisms presented in the previous section (2.2), it becomes clear that, with the transition from mechanical locks to smart systems powered by artificial intelligence and machine learning algorithms, we are witnessing advances in hardware technology and even the evolution of security needs in a more complex environment. While traditional locks focused on physical security through material strength and mechanical design, modern access control systems now focus on adaptability, user identity verification, and the ability to digitally track access. Access control systems have evolved to meet complex operational requirements and can now be classified into three broad categories: PIN, smart card (or magnetic strip), and biometric. Each category represents a new step in the development of secure access: knowledge-based security (PIN), possession-based security (card), and provenance-based security (biometric).

3.3.1 PIN-Based Systems

Personal Identification Number (PIN)-based access control systems are among the oldest digital authentication mechanisms. Due to the memorization of the PIN, this number allows for user authentication. PINs are commonly used in homes, as a form of access control for various offices, and in various financial services, such as ATMs. Due to their low cost and rapid implementation, PINs are attractive for small and medium-sized applications [65]. However, their reliance on the confidentiality of the PIN in a rapidly delivered token poses significant vulnerabilities. These vulnerabilities include vulnerability to PIN theft, shoulder swiping, brute force attacks, and the inability to verify identity based on the PIN alone, as this process relies solely on knowledge of the PIN. Furthermore, PIN-based access control systems offer only limited options, as PINs are not tracked or protected against unauthorized sharing, making them unsuitable for environments that require the security of critical services or the provision of an audit trail [66].

Figure 3.1: PIN-Based System [92]

3.3.2 Keycard Systems

Keycard systems represent a shift in access control from knowledge-based to ownership-based authentication. These systems use magnetic, RFID, or NFC chips embedded in a card or key fob to grant access to a secure location. Keycards can be centrally managed and easily reprogrammed, making them particularly suitable for medium- and high-security environments, including hotels, business offices, hospitals, and educational institutions [67]. The ability to maintain audit trails improves accountability in a keycard system, and they can be easily scaled to include large numbers of employees, patients, or visitors. On the other hand, lost, stolen, or cloned keycards pose security issues. Keycards also require periodic support for card readers and the back-end system, which increases operational maintenance costs [68]. Despite all of these inherent problems with keycard systems, keycard systems have significantly improved access identification and management for a large segment of the population.

Figure 3.2: Keycard System [93]

3.3.3 Biometric systems

Biometric systems are the latest technology in access control. Biometric systems authenticate users based on unique biological or behavioral physiological characteristics, such as fingerprints, facial geometry, iris structure, or voice. Biometric systems have advantages in accuracy and can also be useful in eliminating concerns about lost or stolen credentials and in allowing contactless access, which may be a priority in health-sensitive environments such as hospitals, airports, or public transportation sites [69]. Biometric systems also improve accountability because biometric features are unique, making identity theft more difficult. However, concerns remain regarding data breaches, spoofing attacks using fake biometric features, and ethical concerns regarding consent. The costs and complexity of building a secure biometric system pose barriers to adoption in some contexts [69].

Figure 3.3: Biometric system[92]

This classification of access control principles demonstrates the tremendous leaps that security technologies have made, from the mechanical locks used by ancient societies to intelligent systems that perform dynamic, personalized, and tamper-resistant security authentication. In the following sections, we will discuss how these technologies can be integrated into a sophisticated intelligent security system, and then highlight the development and deployment of template-based access control systems using facial recognition technology.

3.4 Artificial Intelligence (AI) and Facial Recognition in Access Control

As mentioned in Section 2.2, door locks have evolved from purely mechanical systems to modern locks that are electromechanical or biometric in nature. Accordingly, Section 2.3 discussed different types of access control classifications, such as PIN-based systems, keycard systems, and biometric systems. Among these systems, facial recognition is a particular type of biometric system, and has found particular benefits due to its contactless nature, real-time calculations, and accuracy with smart systems.

Artificial intelligence (AI) is an integral part of this transformation process. It is defined as a branch of computer science dedicated to developing machines that exhibit human-like capabilities to perform tasks requiring human cognition (e.g., perception, reasoning, and judgment [70, 71]). When AI is combined with access control systems, traditional security infrastructures can evolve into adaptive, prescriptive, and highly autonomous security systems. AI also facilitates the integration of facial recognition-based systems into platforms such as the Raspberry Pi equipped with camera modules, producing efficient, low-cost, and intelligent alternatives to door locks. Figure 2.4 illustrates the basic components of an AI-enabled system.

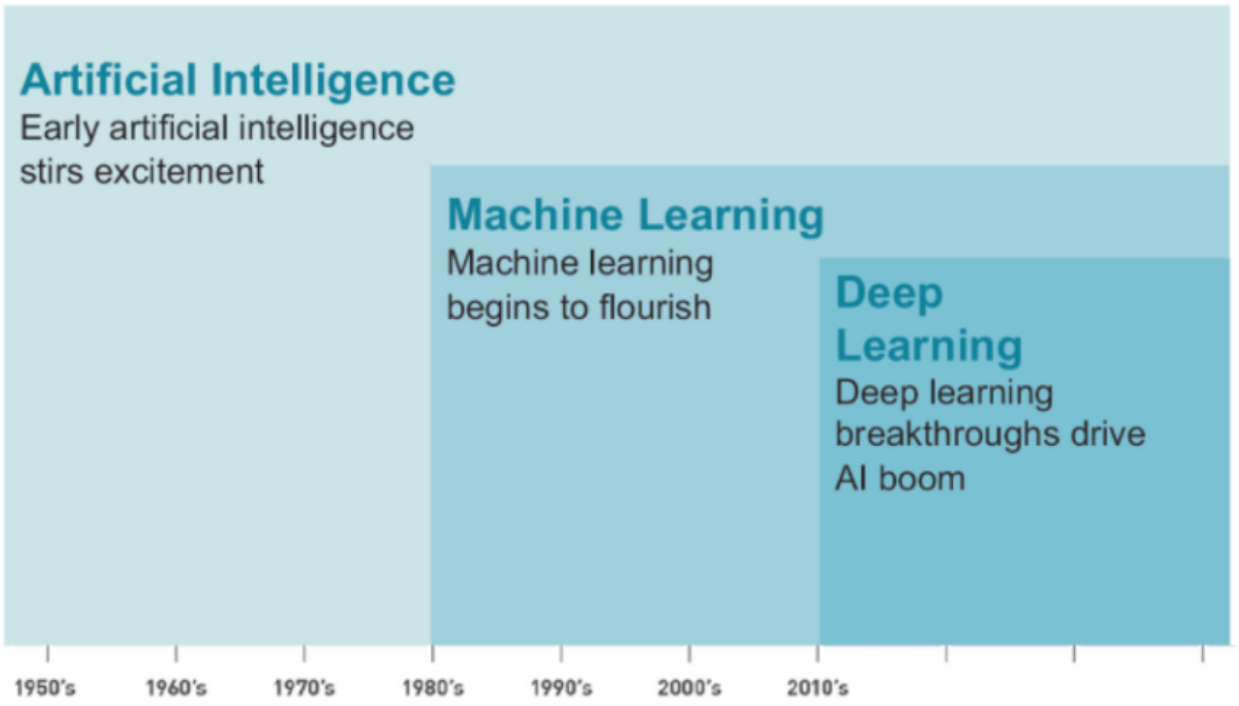

Figure 3.4: Artificial Intelligence [51]

In this section, we elaborates three key subfields of AI: machine learning (ML), deep learning (DL), and transfer learning (TL), and their contributions to the development and application of facial recognition-based access control systems [20]. These models improve recognition accuracy, and improve energy and computational performance compared to available hardware and data.

3.4.1 Machine learning

Machine learning (ML), a fundamental component of artificial intelligence, enables systems to automatically learn from data, detect patterns, and make decisions without the need for explicit programming. In the context of access control, machine learning provides dynamic updating of facial recognition systems, responding to new facial inputs, lighting changes, and changes in facial characteristics [73]. Several ML methods, including k-nearest neighbor (k-NN) [74] and support vector machines (SVMs) [74], have enabled the successful implementation and design of early facial recognition systems and provide some of the most powerful classifiers based on the features generated by the recognition system. Traditional ML methods rely on handcrafted features and are subject to imperfect generalization. These legacy methods are likely to become obsolete, as ML-based models with deep learning capabilities offer opportunities for higher accuracy and scalability [75].

3.4.2 Deep Learning

Deep learning (DL), which uses multi-layer artificial neural networks (or "deep" architectures), is often considered a subfield of machine learning (ML). At its core, deep learning involves using multi-layer neural networks to automatically learn the parameters of nonlinear representations of complex data. Deep learning approaches typically have the ability to learn complex patterns present in data through hierarchical abstractions. This type of approach has numerous applications, but is most common in facial recognition, speech processing, and autonomous navigation [76]. In facial recognition-based access control, the popularity of deep learning models is largely due to their high accuracy and flexibility. The most common deep learning architecture is the convolutional neural network (CNN), which differs from traditional neural networks in its unique ability to analyze objects within a networked data structure, such as images. CNNs operate using learnable filters for a given input image to recognize spatial hierarchies, ranging from low-level features, edges and textures, to high-level representations, facial features and shapes [**?**, **?**].

In recent years, ImageNet-trained CNN models, such as VGGNet, ResNet, and MobileNet, have demonstrated outstanding results on face recognition tasks in both real-time and non-real-time environments. An example is MobileNetV2, which has been successfully used in resource-constrained environments such as Raspberry Pi boards, enabling the development of smart lock systems at a reasonable cost [77].

Deep learning models are often not limited to classification problems, but also include regression problems that require predicting a continuous outcome. For example, we can build a deep learning model that predicts the distance between detectors and the distance between detected facial landmarks, or weight the model's predicted outputs as confidence scores for identity matching. This means that even when true positives for a face are unreliable due to, for example, lighting or occlusion issues, facial recognition systems are able to provide strong and immediate authentication, regardless of some of the challenges a security officer may face. In fact, we can classify these examples as "common challenges" [78].

By incorporating it into an AI architecture (see Section 2.4), deep learning+ not only improves recognition performance but also improves the system's ability to generalize to unseen individuals, potentially leading to lower false acceptance/rejection rates. For this project, I implemented the multi-task cascade convolutional network (MTCNN) algorithm as a face detection method that is robust to lighting, occlusion, and pose [79]. For the recognition component, I implemented the InceptionResNetV1 architecture in the FaceNet framework, which transforms face images into 128-dimensional embeddings, storing the images in a database for efficient face matching and verification, requiring only Euclidean distances [79].

The power of deep learning lies not only in its high levels of accuracy or the ability of a deep learning model to model complex features such as complex facial structures, but also in its ability to achieve this with limited error in terms of perfect matching between the identifier and the face. However, the problem is that building, training a deep learning model, if done from an untrained or unknown instance, is computationally expensive, and requires many data, which is why transfer learning is the justification.

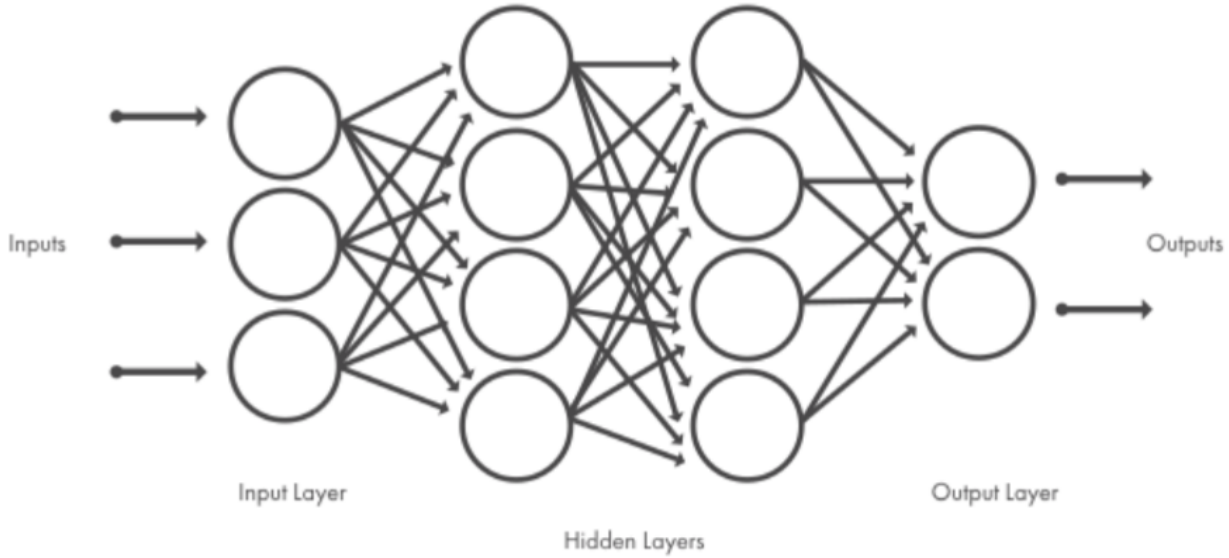

Figure 3.5: Deep Learning [94]

3.4.3 Transfer Learning

Transfer learning is a powerful machine-learning paradigm in which a model trained on a specific source task is deployed as a starting point to learn a different but similar target task. Instead of training a deep learning model from scratch, transfer learning uses pre-trained models that have already learned low- and high-level features from large datasets such as ImageNet or VGGFace2 [80]. These generalizable features can then be further fine-tuned for the target application, which may be faces in access control systems, where labeled data is typically sparse.

In the case of AI-enabled door security, transfer learning offers significantly better performance than CPU-based or embedded systems, reducing the time and data required to train the system. For example, face-embedding models such as InceptionResNetV1, pre-trained on VGGFace2, can be applied to adequately represent features, and then fine-tuned using some face images from air-gapped family members of authorized users, to provide fast , accurate verification authorized users' faces in embedded systems such Raspberry Pi [81].

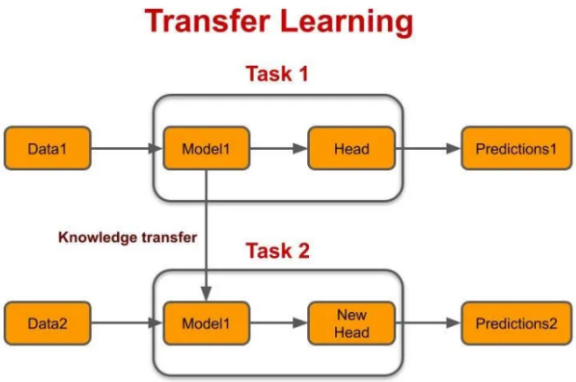

Figure 3.6: Transfer Learning[96]

3.4.3.1 Types of Transfer Learning :

Transfer learning strategies can be broadly classified into the following types, depending on the relationship between the source and target domains and tasks [82]:

- **Inductive Transfer Learning:** the source and targeted areas will be the same as the tasks differ. Consequently, the form will be adjusted using the data called for the target task (such as adjusting the general facial recognition form, on a safety system with new identities) [83].
- **Transductive Transfer Learning:** the tasks will be the same as the areas differ. In this case, the form of knowledge from the source field (such as a model that is trained to celebrities) will be applied to the same task (i.e. face recognition) in a new field (i.e. employee's faces) [83].
- **Unsupervised Transfer Learning:** the tasks and domains will differ, and there is no labelled data available in either task, or domain. In this case, the model will learn through extracting some kind of structure from unlabeled data. An example of this type of learning may complain anomaly detection or using an unsupervised clustering approach to cluster facial feature points in the absence of previously issued labels for any of the features [83].

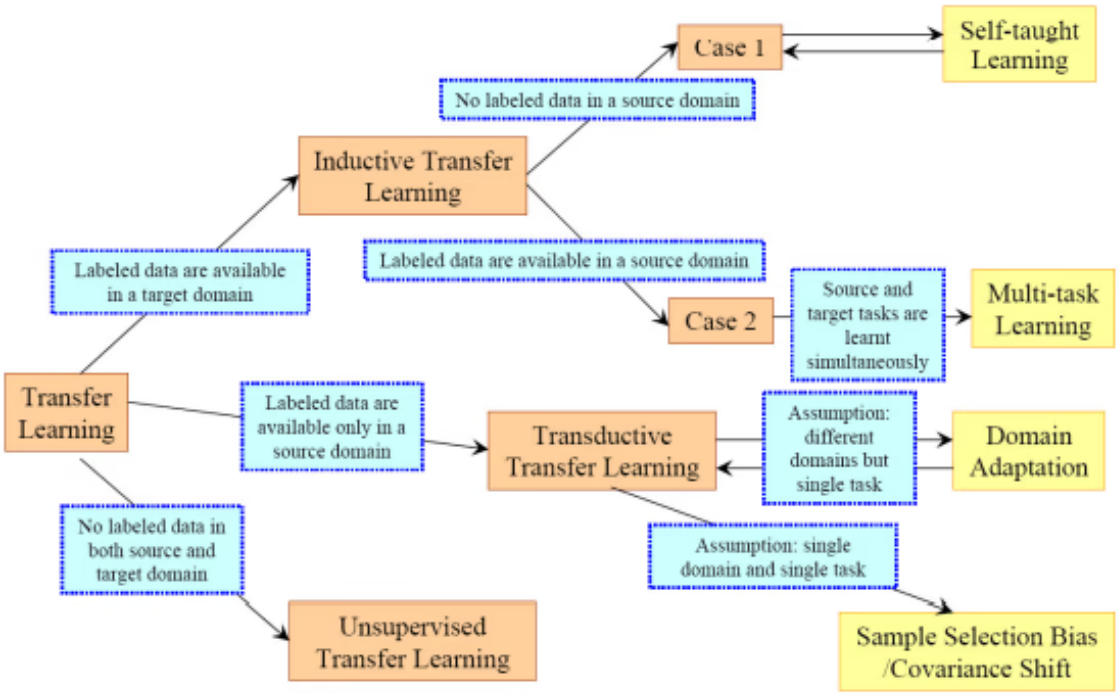

Figure 3.7: Types of Transfer Learning [95]

3.4.3.2 Mechanism of Transfer Learning

In a general multi-stage transfer learning process, a machine-learning model can share learned knowledge from a source task to an entirely different target task. The first step is selecting a base model that has been pre-trained on a much larger and diverse dataset (e.g., through datasets such as VGGFace2, ImageNet, etc.) that will give it a prior understanding of how to extract relevant features from data; in this first step, the model has already learned to extract characteristic features about data such as edges, textures , and shapes[84].

The second step is layer freezing. The early layers of the pre-trained model are usually frozen and left untouched. These layers usually correspond to the low-level features found in most tasks (visual tasks at least). The following step is to fine-tune the regions of the model toward patients in the context of a specific domain (e.g., a dataset with facial images of challenged individuals). This fine-tuning would give the model the capacity to learn new representations while at the same time retaining general optimal representations it acquired in the prior layers [84].Finally, the optimized model is implemented in the operational environment. In the case of this work, it is implemented in a real -time access control system using a Raspberry Pi module and the camera to provide high recognition accuracy with a very low calculation load, which makes it suitable for integrated and on board IT [84].

Finally, the optimized model is implemented in the operational environment. In the case of this work, it is implemented in a real -time access control system using a Raspberry Pi module and the camera to provide high recognition accuracy with a very low calculation load, which makes it suitable for integrated and on board IT [84].

3.4.3.3 Frozen vs. Trainable Layers

In Transfer Learning, two main components help in adapting models effectively:

Frozen Layers: These layers from a pre-trained model remain unchanged during fine-tuning. They retain general features learned from the original task, extracting universal patterns from input data.

Trainable Layers: These layers are adjusted during fine-tuning to learn task-specific features from the new dataset,allowing model to meet the new tasks unique requirement[97]

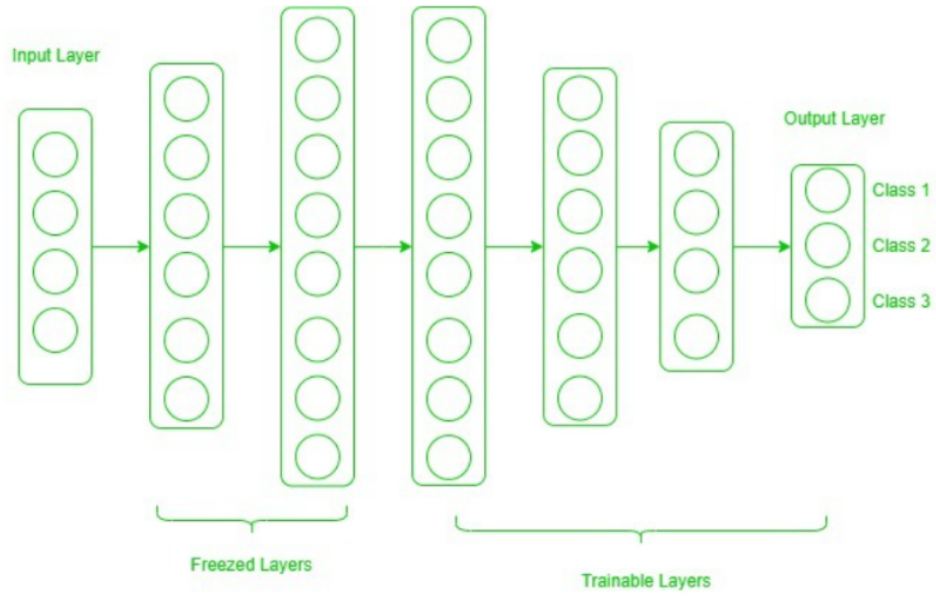

Figure 3.8: Frozen vs. Trainable Layers [97]

3.4.3.4 Use Cases Environments

Here are some situations where transfer learning can be particularly effective:

Limited Data:

Transfer learning can be useful when you only have a small amount of data available to train a model because the pre-trained model already has knowledge of the domain and can be used to enhance the model's performance.Transfer learning can be used to modify a pre-trained model to your specific job and boost its accuracy, for instance, if you want to categorize photographs of rare animals but only have a small number of labelled images.

Low Computing:

Starting from scratch while training a deep neural network can be time- and resource-consuming.By starting with a pre-trained model that has already picked up useful features and then customizing it for your particular activity, transfer learning can be utilized to save time and resources.

New Domains:
When you want to apply machine learning to a new domain you have limited knowledge of, transfer learning can leverage the expertise of pre-trained models that have already learned about the domain.

For example, suppose you want to classify medical images but need more expertise in the medical field.In that case, you can use transfer learning to adapt a pre-trained model that has already learned useful features in the medical domain.

Overall, transfer learning can be a powerful approach for machine learning practitioners who want to leverage existing knowledge and resources to solve new problems.[98]

3.4.3.5 Applications of Transfer Learning

Transfer learning is widely used across multiple domains, including:

Computer Vision: Transfer learning is prevalent in image recognition tasks, where models pre-trained on large image datasets are adapted to specific tasks such as medical imaging, facial recognition, and object detection.

Natural Language Processing (NLP): In NLP, models like BERT, GPT, and ELMo are pre-trained on vast text corpora and later fine-tuned for specific tasks such as sentiment analysis, machine translation, and question-answering.

Healthcare: Transfer learning helps develop medical diagnostic tools, leveraging knowledge from general image recognition models to analyze medical images like X-rays or MRIs.
Finance: Transfer learning in finance assists in fraud detection, risk assessment, and credit scoring by transferring patterns learned from related financial datasets.[97]

3.4.3.6 Benefits of Transfer Learning

- **Faster Training:** Since the model has already learned general features from the pre-training phase, it requires fewer iterations to adapt to the new task. This significantly reduces the time and computational resources needed for training.[96]
- **Less Data Dependency:** Transfer learning can be particularly advantageous when you have a limited amount of data for your specific task. The pre-trained model has already learned useful features from a large dataset, which can be applied to your smaller dataset.[96]
- **Enhanced Performance:** Starting with a pre-trained model, which has already learned from substantial data, allows for faster and more accurate results on new tasksideal for applications needing high accuracy and efficiency.[97]

- **Time and Cost Efficiency:** Transfer learning shortens training time and conserves resources by utilizing existing models, eliminating the need for training from scratch.[97]

3.4.3.7 Limitations and Challenges

Domain mismatch: The pre-trained model may not be well-suited to the second task if the two tasks are vastly different or the data distribution between the two tasks is very different.
Overfitting: Transfer learning can lead overfitting if the model is fine-tuned too much the second task,it may learn task-specific features that do not generalize well to new data.
Complexity: The pre-trained model and the fine-tuning process can be computationally expensive and may require specialized hardware. [97]

3.4.4 Differences between Deep Learning and Transfer Learning

Deep learning and transfer learning are two areas of artificial intelligence focused on automating complex pattern recognition. However, they follow fundamentally different paradigms. Deep learning relies on training a brand new neural network from scratch, using datasets that are extensive, fully-labelled, and employing compute resources that may be costly and difficult to obtain. Scaling deep learning is financially and temporally expensive, but results in specialized models that are optimized for specific domain applications [39].

Transfer learning, on the other hand, is an area of AI that accepts the heavy burden imposed by large datasets and fast compute performance in the unstructured world of AI, and attempts to avoid some of the these for the most part inconceivable, expensive and difficult demands by allowing learners to access pre-trained models, that were originally previously-trained on large and generic datasets. Pre-trained models allow learners to absorb the base framework, and learn more with few data points related to a task that is associated with the new task they are learning to do experimentally. After acquiring a few related data points, learners can explore or "fine-tune," the pre-trained model for a copy of the model relative to the new task and label data.

Transfer learning is particularly useful for situations when creating an extensively wore double and labelled dataset are impractical (e.g., access control systems that are trained on a facial recognition technique that is deployed in real-time at an edge device or edge computing device) [85].

Given the speed, flexibility, and reduced training requirements associated with transfer learning, it is clearly the learner's preferred approach to apply AI concepts for embedded applications and applications implemented in the real-world context - all of which are critical frameworks for accuracy, speed and reduction in resource consumption [85].

3.4.5 AI in Security Systems

Artificial Intelligence (AI) is fundamentally changing the nature of security systems by offering intelligent capabilities beyond past systems limited by rules. AI-based models can enable security systems to perform predictive analysis, adapt to different environments, and make decisions independently and instantaneously. This is revolutionary for biometric authentication systems, particularly AI-enabled facial recognition, where AI models support facial recognition and authentication systems by adding features such as spoof detection, liveness detection, and changing environmental states/conditions (lighting or occlusion) [86].

Recent studies in the industry show the impact of AI, which strengthens the conversation around the cost of a data breach. The IBM Cost of a Data Breach Report (2023) found that organizations that implement significant AI and automation tools reduced their average time to contain a breach by 108 days. They also saved about USD 1.76 million in responding to a data breach event compared to organizations who were not using AI. These statistics show the effect of AI on operational effectiveness and financial efficiency [87].

The increasing market potential relates more ways AI is being recognized. The global market for AI in security is expected to grow from USD 20.19 billion in 2023 to USD 141.64 billion by 2032, with a compound annual growth rate of 24.2% [87]. This increased growth shows the growing need for intelligent and automated solutions across many areas, including critical infrastructure, enterprise security, and smart home uses.

In the field of access control, AI facial recognition technology has quickly become a fundamental application. By deleting the need to contact and provide real -time identification processes, it allows a pleasant user experience without compromise to security. AI facilitates variability and adaptive reasoning (that is to say people, vehicles and the environment), leading to evolutionary and precise authentication. Thus, these systems can be used in environments ranging from office buildings and government buildings to intelligent condominiums and buildings.

3.5 Detect eye blinking in videos :

In face recognition door access systems, eye blinking detection is used as a liveness verification method to prevent spoofing attacks with photos or videos. By analyzing facial landmarks around the eyes, the system calculates **the Eye Aspect Ratio (EAR)** to measure eye openness. A blink is detected when the EAR drops below a certain threshold and then quickly returns to normal, indicating natural eye movement. This ensures that only live individuals not static images or or 3D masks can trigger face recognition and gain access.

useing facial landmark detection to detect specific 68 points on the face show in Figure 3.9. This post is inspired by the folowing posts which are further modified and improved: [116] and [117].

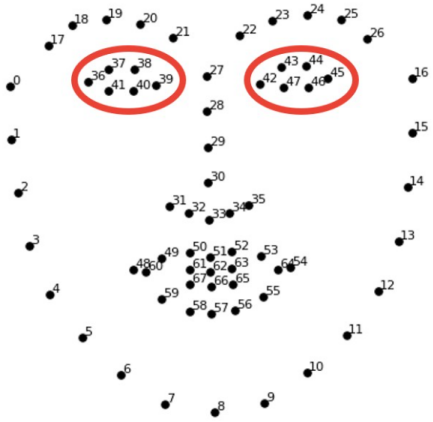

Figure 3.9: 68 land marks [118]

By knowing the indexes of these points, we can use the same method and select a specific area of the face (e.g. eyes, mouth, eyebrows, nose, ears). To create an eye blink detector, eyes will be the area on the face that we are interested in. We can divide the process of developing eye blink detector into following steps:[118]

1. Detecting the face in the image
2. Detecting facial landmarks of interest (the eyes)
3. Calculating eye width and height
4. Calculating eye aspect ratio (EAR) relation between width and the height of the eye
5. Displaying the eye blink counter in the output video

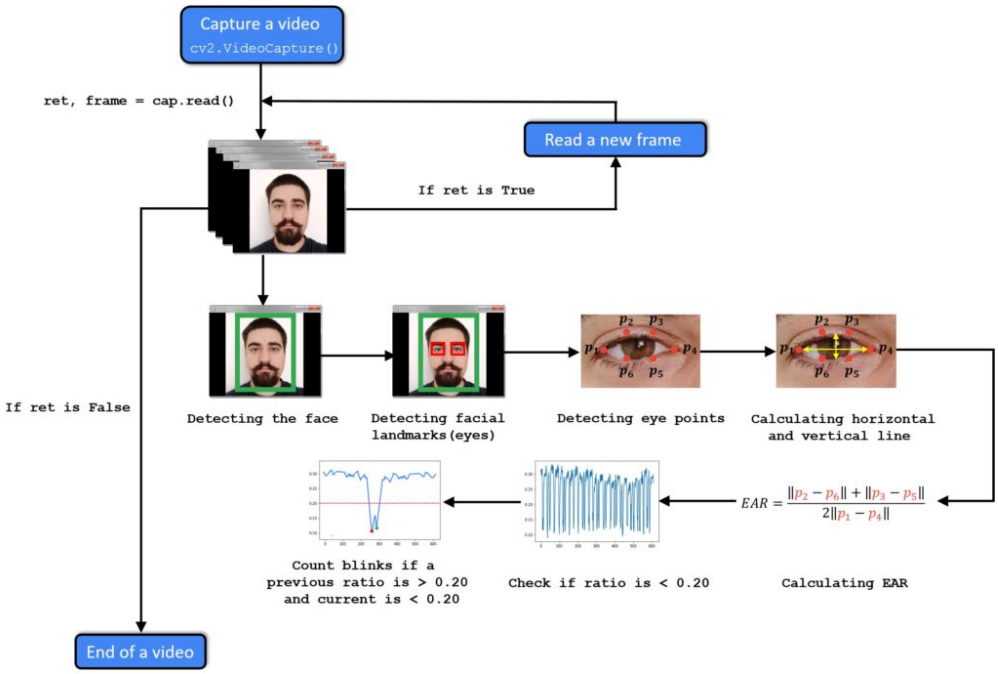

Figure 3.10: Schematic of how the blink detection work [118]

3.5.1 Definition of EAR :

Real-Time Eye Blink Detection using Facial Landmarks is the research paper published in 2016 by Tereza Soukupova and Jan Cech from the Faculty of Electrical Engineering, Czech Technical University in Prague. Authors developed a real-time algorithm to detect eye blinks in a video sequence. A key part of this algorithm is the eye aspect ratio (EAR) which can be used to determine whether a person blinks or not in the given video frame. For better understanding of this concept, let us look in the following image.[118]

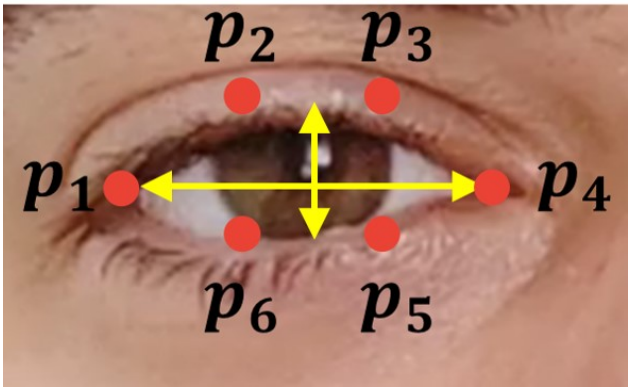

Figure 3.11: EAR in EYE [118]

In this Figure 3.11 we can see the eye which is represented by a set of 6 labeled facial points with specific coordinates. Horizontal line is distance between points p1 and p4 (width of an eye), and vertical line is distance between middle of points p2 and p3 and middle of points p6 and p5 (height of an eye.) The length of the horizontal line will always be a constant, while the length of the vertical line will change depending on the opening and closing of the eye. We can detect blinking by calculating the length of these two lines and then finding the ratio between them. This ratio will be approximately constant while the eye is open, and it will quickly fall to zero when a blink occurs.[118]

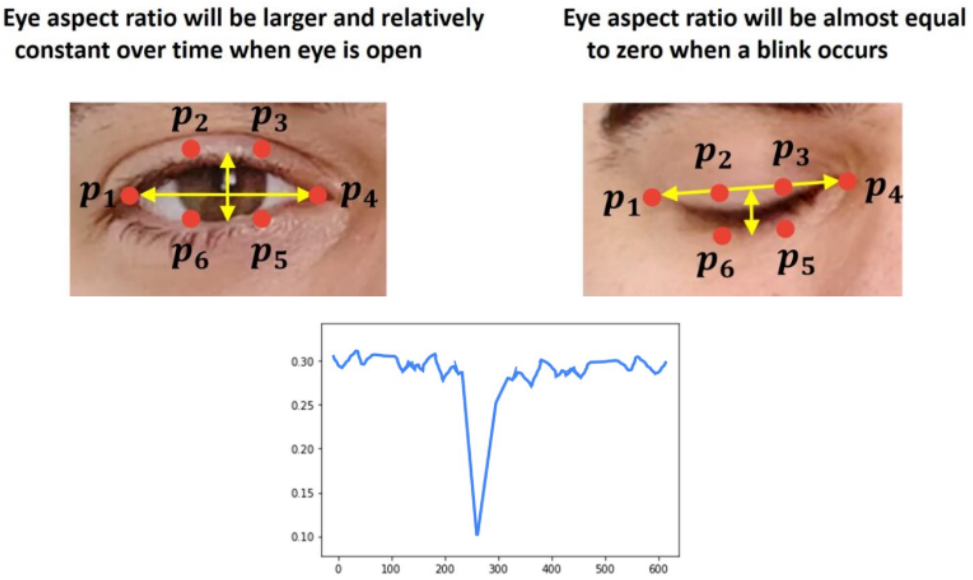

Figure 3.12: EAR [118]

In the Figure 3.12 on the left we can see that aspect ratio will be larger and relatively constant over time. On the other hand, in the second image we can see that aspect ratio will be almost equal to zero which indicates that the person is blinking at that moment.[118]
We can calculate the aspect ratio with the following equation:

$$\frac{\|p2 - p6\| + \|p3 - p5\|}{2\|p1 - p4\|} = EAR \tag{3.1}$$

3.6 Internet of Things (IoT):

The Internet of Things (IoT) is a new technology defined as a worldwide network of interconnected machines and devices. These devices can collect and share data, fostering automation and real-time insights. To deploy effective IoT-based products and services, five essential technologies are commonly used :

- Sensor Networks: these networks consist of interconnected devices that collect and transmit data
- Data Communication: wireless technologies like Radio Frequency Identification (RFID) enable efficient data transmission between devices within the network.
- Data Processing and Management: middleware acts as a bridge between sensors and applications.
- Cloud Computing: cloud platforms provide the necessary infrastructure and resources to store, analyze, and manage the vast amount of data generated by IoT devices.
- Application Software: specialized software applications are designed to interpret and use the collected data [**?**]

3.6.1 Role of Raspberry Pi in IoT Systems

The Raspberry Pi, a low-cost, compact single-board computer developed by the Raspberry Pi Foundation, is a critical component in edge computing in Internet of Things (IoT) architectures. With its quad-core processing capabilities, GPIO (General Purpose Input/Output) pins, and Linux-based OS, it is a popular choice for prototyping and deploying embedded applications [88].

In an access control system, the Raspberry Pi acts as a local control unit that interfaces with biometric sensors (e.g., cameras for facial recognition), and then acts as an actuator for locks based on the results of the authentication. The Raspberry Pi is continuously in a low-power state, affordable, and supports the implementation of an AI model. Therefore, it is particularly suited for real-time facial recognition systems where hardware is constrained to as little power and cost as possible [88].

The Raspberry Pi is an open-source platform, which allows integration with cloud services and machine learning frameworks to build intelligent security systems.

3.6.2 IoT-Based Smart Access Control Architecture

Internet of things is a foundation of the new IoT access control system commonly known as intelligent door locking systems. In this system, every lock, lock access controller, card reader, and other associated devices are assigned an unique IP address, which is used for the device communication [89].

In a single framework, different smart devices are usually connected through wireless networks to their managing software at the center or mobile apps. The applications can be configured for automatic and manual control of different locks and controllers. Moreover, the security alerts and notifications can also be configured to receive on mobile apps in real-time[89].

Each machine/device is configured for its operating conditions, criteria, sensitivity and authority in core management control software, which is utilized as controller of the entire system. A copy control of this system is utilized as mobile app on your mobile devices too; you can obtain status of your access system and you can also issue instructions from your app. Any unauthorized activity in your access system generates an alert and detailed notice on your primary management software controller or mobile application [89].

3.6.3 Advantages of IoT in Access Control

By integrating the Internet of Things (IoT) with access control systems, physical security management and surveillance have reached an entirely new level. IOT compatible solutions demonstrate several technical and operational advantages compared to traditional access systems which strengthen both security and conviviality [89]. The main advantages are described as follows:

3.6.3.1 Remote Accessibility and Real-Time Monitoring:

Through mobile applications and web dashboards users can remotely manage and monitor IoT-based access control systems. Through this means, administrators maintain the capability to adjust user access permissions immediately from any location. The system enables real-time tracking of entry logs, which facilitate instant responses to unauthorized access attempts [89, 90].

3.6.3.2 Automated Decision-Making:

The AI-based data analytics systems operating within IoT platforms execute decision-making functions based on established rules and behavioral guidelines. The system operates by blocking unauthorized access and restricting entry during non-approved timeframes [44].

3.6.3.3 Enhanced Security through Real-Time Alerts:

The IoT-enabled security systems send immediate warnings to their users whenever security violations such as entry without permission or equipment manipulation or forced entry takes place. Security personnel receive real-time alerts through SMS messages and email notifications and mobile application notifications which help them react promptly and understand the situation better [**?**, 90].

3.6.3.4 Customization and Multi-Level Access:

These systems provide detailed management of user permissions by creating distinct security levels and responsibilities for different roles. Restricted zones in organizations can maintain controlled access for specific personnel groups while allowing unrestricted entry for other staff members, which enhances the security management of internal environments [90].

3.6.3.5 Efficient Audit Trails and Data Logging:

The IoT system maintains continuous tracking of user interactions together with equipment conditions and operational data. The recorded activity details function as an audit trail which promotes transparency and makes it easier to meet compliance standards while providing valuable information for security investigations during breach incidents [**?**, 90].

3.6.3.6 Cost-Effectiveness and Maintenance Optimization:

Through IoT-based access control systems, organizations achieve long-term cost reductions since they eliminate traditional key management while reducing manual supervision and enabling maintenance through system health monitoring [90].

3.6.3.7 Integration with Other Smart Systems:

The synchronization between IoT access controls and building automation systems enables coordination with lighting systems as well as HVAC and fire alarm systems. The system enables door unlocking to trigger hallway light activation and security alarm deactivation automatically thus enhancing user satisfaction and power conservation [89].

3.7 Conclution

The accuracy and reliability of face recognition technology cannot meet the requirements in some fields for the time being. At this stage, the significance is to liberate those who have been in the repetitive working environment for a long time, to achieve the purpose of reducing cost and enhancing efficiency, Still, it does not mean to replace a certain profession or technology. With the development of pattern recognition, computer vision, image processing and machine learning, the accuracy and speed of face recognition will be improved.

Just like computers can surpass human beings in many fields through deep learning, machine vision cooperates with databases and processors in the background through advanced devices in the front end, and computer face recognition will surpass human recognition speed and accuracy in an all-round way. In addition to identity recognition, it will also realise new functions such as judging age, beauty and health. Shortly, face recognition technology will gradually come into daily life and be widely used. In the name of safety, for public places such as subway, where people flow in and out on a large scale daily, the first physical examination is carried out. Then the same examination of people is carried out. Now face recognition is to be carried out. Shortly, gene or fingerprint recognition may be further carried out. If it develops according to the current trend, there is such a possibility.

In the near future, public transportation such as subway will become a kind of privilege that only some members of society can enjoy. If this society has not yet fallen into the state of persecution delusion, it should stop at security issues. What hysterical pursuit of security brings to society is not security at all, but comprehensive repression and panic. For the subway to use face recognition for classified security check, the real worry and fear are that their information is abused by the public authority. Because when they abuse, people have no idea what kind of price they and their families will pay.

Chapter 4

Design and implementation

4.1 Introduction

As there is a growing need for smart and effective security systems, the need to develop modern access control solutions with biometric recognition technologies has arisen. Facial recognition systems are some of the most prominent solutions that provide security with convenience, in contrast to traditional systems such as cards or passwords that can be lost or stolen.

This chapter covers the design and implementation of our suggested access control system that employs facial recognition technology, on a camera, Raspberry Pi module, and sophisticated artificial intelligence algorithms. The system also incorporates liveness detection and anti-fraud mechanisms, along with an interactive web interface for easing user management and real-time activity monitoring.

4.2 Architecture of System

The architecture of the proposed face recognitionbased door access system is built to ensure secure and real-time access control using a combination of embedded hardware and deep learning models. The Raspberry Pi is used to detect the presence and distance of a person, while the cameraconnected directly to the servercaptures the video feed. When a person is within the allowed range, the system begins detection using YOLO to filter spoofing attempts from screens or phones. If valid, facial recognition is performed using MTCNN and FaceNet, along with liveness detection via eye blinking. All results are managed through a Flask-based web interface that allows live monitoring, access control, data management, and alerts.

Figure 4.1 illustrates the entire architecture of the system, from sensor activation to intelligent decision-making and remote control.

4.2.1 Component Diagram of the system

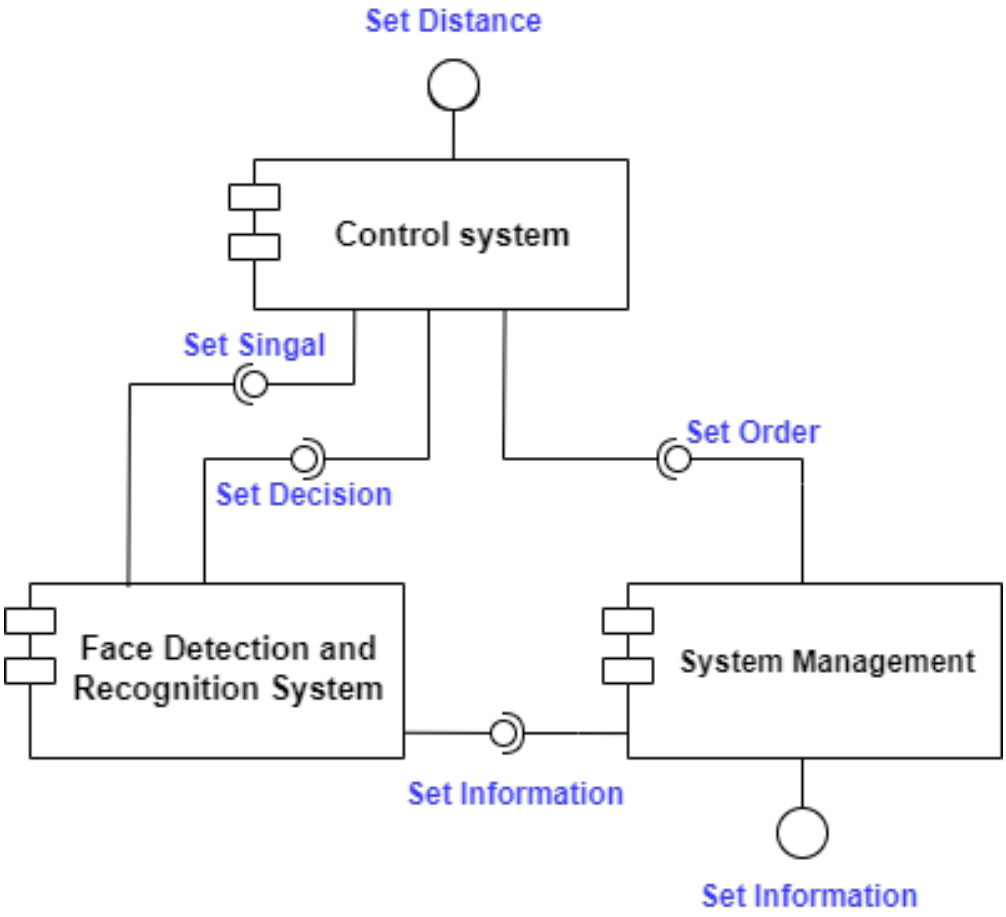

Figure 4.1: component diagram for system

Explanations

Input: A facial image captured in real time by the camera

Output: An access decision (door unlock or deny) based on facial recognition and user permission status.

The structure of the system, named VeriFace Gate, is shown in Figure 4.1 It includes the following three main components:

System Management: saves logs,Manage Faces, and communicates with the Raspberry Pi and via TCP/IP.

Control system: Includes the Raspberry Pi which receives access decisions, controls the electronic lock, and interacts with the LCD screen, buzzer, and LEDs for physical access feedback.

Face Processing Module: Responsible for capturing the facial image, detecting the face using MTCNN, verifying liveness through blink detection and screen spoof detection using YOLOv8s, and finally recognizing the identity using FaceNet.

Detailed description of the system: In this section we will detail the description of each component with activity and use case diagrams.

4.2.1.1 composant 01: System Management

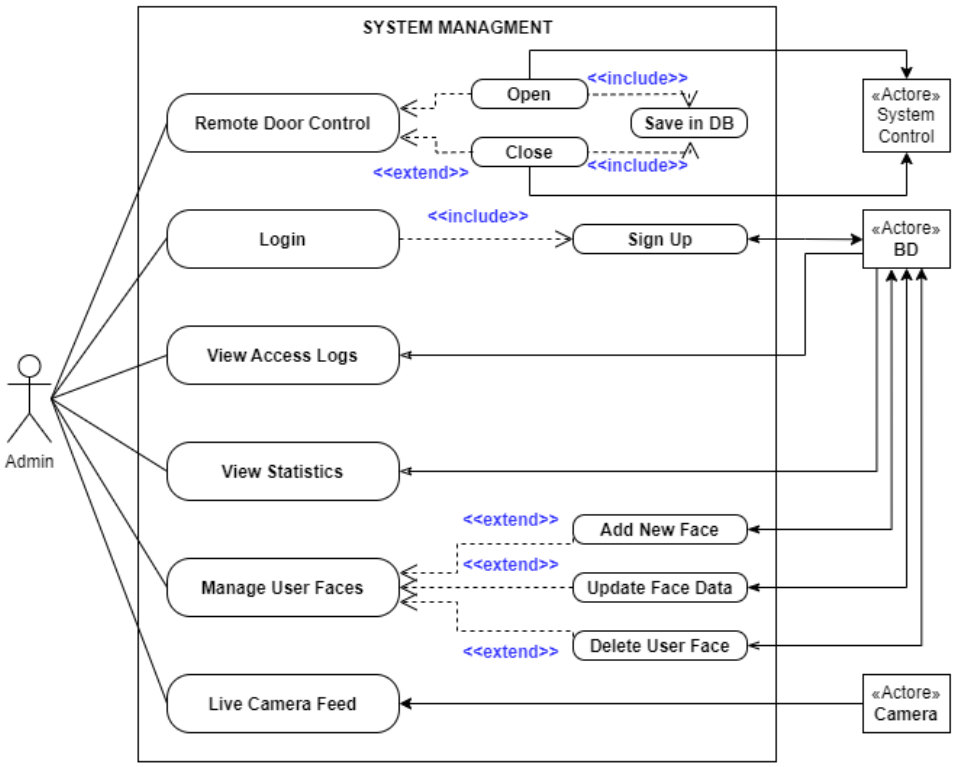

Figure 4.2: USE CASE Diagrammes of System Management

The Use Case diagram above represents the functionalities available to the Admin user within **the System Management** module of the "VeriFace Gate" system. This diagram provides a visual representation of the interactions between the administrator and the system's key features. The system is composed of several use cases, each of which corresponds to a task that can be performed by the administrator.

Main Actor:

- **Admin:** The system administrator who has full control over the platform functionalities, including user management, data analysis, and remote hardware control.

Primary Use Cases:

1. **Remote Door Control** The admin can remotely manage the state of the access control system by executing:
   - **Open:** Unlocks the door remotely.
   - **Close:** Locks the door remotely.
   - Both actions include a call to Save in DB, which stores the event and its metadata (Name, Type, TimeStamp) into the database.

- This use case interacts with the external System Control actor (hardware interface) to perform the actual door control operation.

2. **Login / Sign Up**

   - **The Login:** Allows the admin to securely access the system using their credentials.
   - **The Sign Up** operation is included as part of the login process, specifically for initial setup or registering a new admin. It connects to **the Database (BD)** to create a new admin record.

3. **View Access Logs**

   * Provides access to the historical data of user authentications, access attempts, and system responses. Data is fetched from Database (BD)

4. **View Statistics**

   * Enables the admin to analyze system activity through various metrics and statistical charts (e.g., number of access attempts, access granted/denied ratio). The data source is the Database (BD).

5. **Manage User Faces**

   * A critical functionality that allows the administrator to handle biometric data stored in the system:

   - **Add New Face:** Inserts a new users facial data into the system.
   - **Update Face Data:** Edits the facial record of an existing user.
   - **Delete User Face:** Removes a users facial data permanently.

   * These three functionalities are modeled as extend relationships from "Manage User Faces", meaning they are optional sub-tasks that extend the main use case based on context.

   * All operations are linked to the Database (BD) to ensure data consistency and persistence.

6. **Live Camera Feed**

   *Grants the admin access to real-time video streaming from the surveillance camera, typically used for monitoring or verifying ongoing access attempts. This is directly connected to the Camera video.

This use case diagram provides a comprehensive overview of the functionalities that the system administrator can perform within the VeriFace Gate system. Each interaction is clearly defined, and relationships such as **ńincludeż** and **ńextendż** help modularize and clarify how various system features are related. This logical breakdown ensures maintainability, scalability, and security across the systems operation.

4.2.1.2 composant 02: Control system

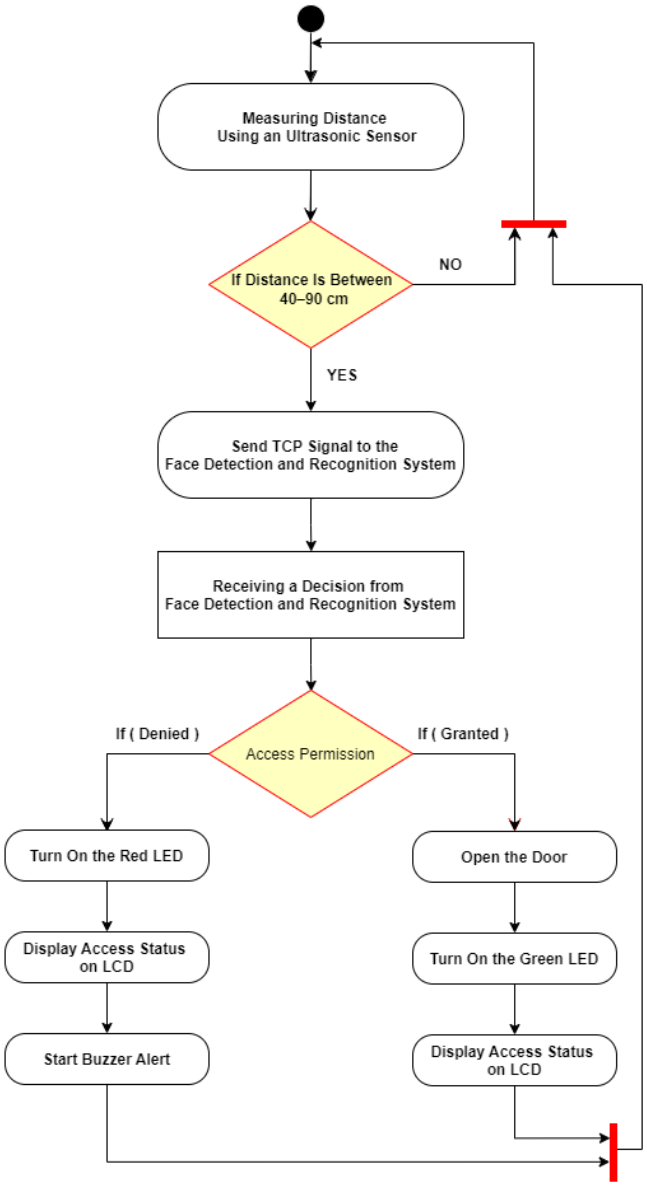

Figure 4.3: Activite diagram for controler system

This UML Activity Diagram represents the dynamic behavior of the VeriFace Gate access control system. It models the sequential flow of control, activities, and decisions based on sensor input and recognition system response.The system utilizes a distance sensor, TCP communication, and hardware feedback components (e.g., LEDs, buzzer, LCD, electric door). It defines the actions required to either grant or deny access.

- **Initial State:**

  The system is in an idle loop, constantly measuring distance using an ultrasonic sensor.

- **Step 1: Distance Verification**

  "Measuring Distance Using an Ultrasonic Sensor": This step checks whether a person is physically present and within the acceptable range.

  Condition Check:

  If the measured distance is between 40 cm and 90 cm, the system proceeds to the recognition step.

  If not in range, the system loops back to distance measurement and takes no further action.

- **Step 2: Trigger Face Detection**

  "Send TCP Signal to the Face Detection and Recognition System": A TCP request is sent to the central server to activate the face detection and recognition process, signaling that a user is present within the allowed range.

- **step 3: Await Recognition Decision**

  The system waits for a response from the facial recognition system, which processes the image and determines whether the user is recognized and authorized.

- **Step 4: Decision Evaluation Access Permission**

  Access Permission Decision:

  If the user is Granted access:

  - The system opens the door.
  - Turns on the green LED as visual confirmation.
  - Displays "Access Granted" on the LCD screen.

  If the user is Denied access:

  - The system keeps the door closed (or closes it if open).
  - Activates the red LED to indicate denial. Shows "Access Denied" on the LCD.
  - Triggers the buzzer to alert nearby personnel of a failed or unauthorized attempt.

- **Final State** The system returns to the initial state, continuously monitoring the environment for new users.

4.2.1.3 composant 03:Face Detection and Recognition System

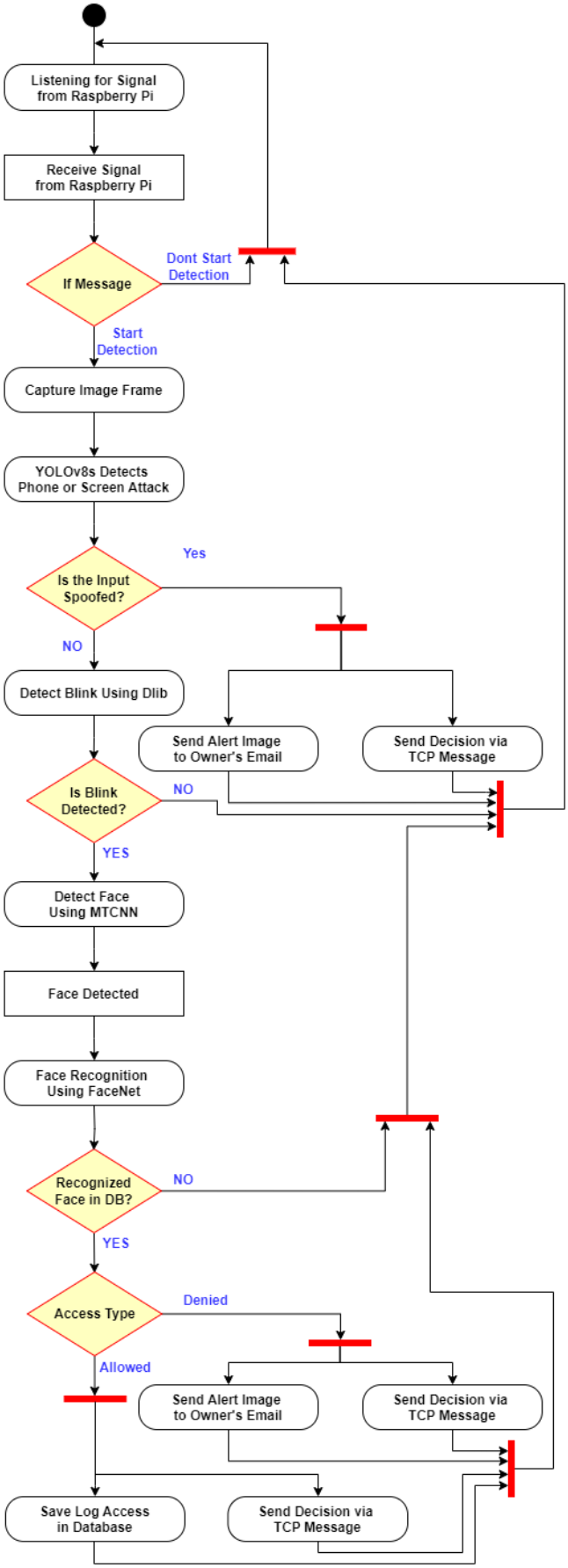

Figure 4.4: Activite Diagrammes of Face Detection and Recognition System

This activity diagram illustrates the operational workflow of our intelligent access control system. It captures the system's behavior from the moment a signal is received from the Raspberry Pi to the final decision of granting or denying access. The diagram highlights key steps such as spoofing detection, blink-based liveness verification, face recognition, and real-time communication via TCP. It serves as a clear visual guide to understand how security, decision-making, and system integration are achieved.

1. **Listening for Signal from Raspberry Pi**
   - The system begins in an **idle state**, actively waiting for a trigger message from the Raspberry Pi.
   - The Raspberry Pi detects human presence via distance sensors and sends a signal when a person is between 40 to 90 cm.
2. **Receive Signal from Raspberry Pi**
   - Upon receiving a valid signal, the server interprets this as a prompt to initiate the facial authentication pipeline.
   - A decision node checks if the message instructs to start or ignore detection.
3. **Message Decision Node**
   - If the message is valid, the system **starts detection.**
   - Otherwise, the process returns to the initial waiting state.
4. **Capture Image Frame**
   - The camera captures a **live image frame** of the person.
   - This image becomes the input for all subsequent analysis.
5. **YOLOv8s Detects Phone or Screen Attack**
   - The image is passed to a **YOLOv8s object detection model**, trained to detect **phones or screens**, which are typical tools used for spoofing facial recognition systems.

Decision Node: Is the Input Spoofed?

- **Yes** –> If a phone or screen is detected, the system:
  - Sends an alert image via email to notify the owner of a spoofing attempt.
  - Sends a TCP message to the control unit indicating a denied access.
  - The process terminates for this session.
- **No** –> Continues to verify liveness using blink detection.

6. **Detect Blink Using Dlib**

   - The system applies blink detection using Dlib's facial landmark detector to check for eye movement, confirming the presence of a live person.

   Decision Node: Is Blink Detected?

   - **No –>** This indicates a static image or video and is treated as **a spoof attempt:**
     - Decision is sent via TCP to deny access.
     - The session ends.
   - **Yes –>** The person is considered live, and detection proceeds to the face detection phase.

7. **Detect Face Using MTCNN**

   - The system now employs **MTCNN (Multi-task Cascaded Convolutional Networks)** to detect the location of a face in the image.
   - This step extracts a **cropped, aligned face image** suitable for embedding and recognition.

8. **Face Recognition Using FaceNet**

   - The extracted face is converted into a **128-dimensional embedding** using **the FaceNet** model.
   - This embedding is then compared to**the database of known faces.**

   Decision Node: Recognized Face in DB?

   - **No –>**
     - The person is unknown.
     - The system sends a TCP message denying access.
   - **Yes –>**
     - The face is found in the database.
     - The system proceeds to check their access permissions.

9. **Access Type Evaluation**

   - Once the user is recognized, their **access type** is checked (Allowed or Denied).

   Decision Node: Access Type

   - **Denied –>**
     - **Sends an alert image via email** to notify the owner of a spoofing attempt.
     - **Sends a TCP message** to the control unit indicating a denied access.
     - The process terminates for this session.
   - **Allowed –>** – Access is granted.

10. **Final Actions on Approval**

- **The system:**
  - Saves the access event in the database (log file including time, name, and decision).
  - Sends a TCP signal to the Raspberry Pi to trigger the door lock mechanism.

This diagrams serves as a backbone of smart, AI-powered biometric authentication, ideal for high-security environments such as research labs, corporate offices, or smart homes. It exemplifies a fusion of hardware-software interaction, network communication, and deep learning-driven decision-making.

General process of the system:

The general process of Face Detection and Recognition System is described as following architecture:

In order to provide a clear understanding of the dynamic behavior of the proposed access control system, the UML Sequence Diagram has been designed and illustrated. This diagram models the chronological interaction between the system components, showcasing the flow of messages exchanged during a typical access request scenario.

It serves as a valuable tool to analyze how objects interact over time, helping to identify potential bottlenecks, validate logic, and ensure synchronization between software modules and hardware components such as the Raspberry Pi, camera, Database, siteweb ,and electric lock. Through this diagram, each step from user detection to access decision and logging is represented in a structured and detailed manner, reflecting the intelligent coordination between the client and server sides of the system.

4.2.1.4 UML Sequence Diagram of The System

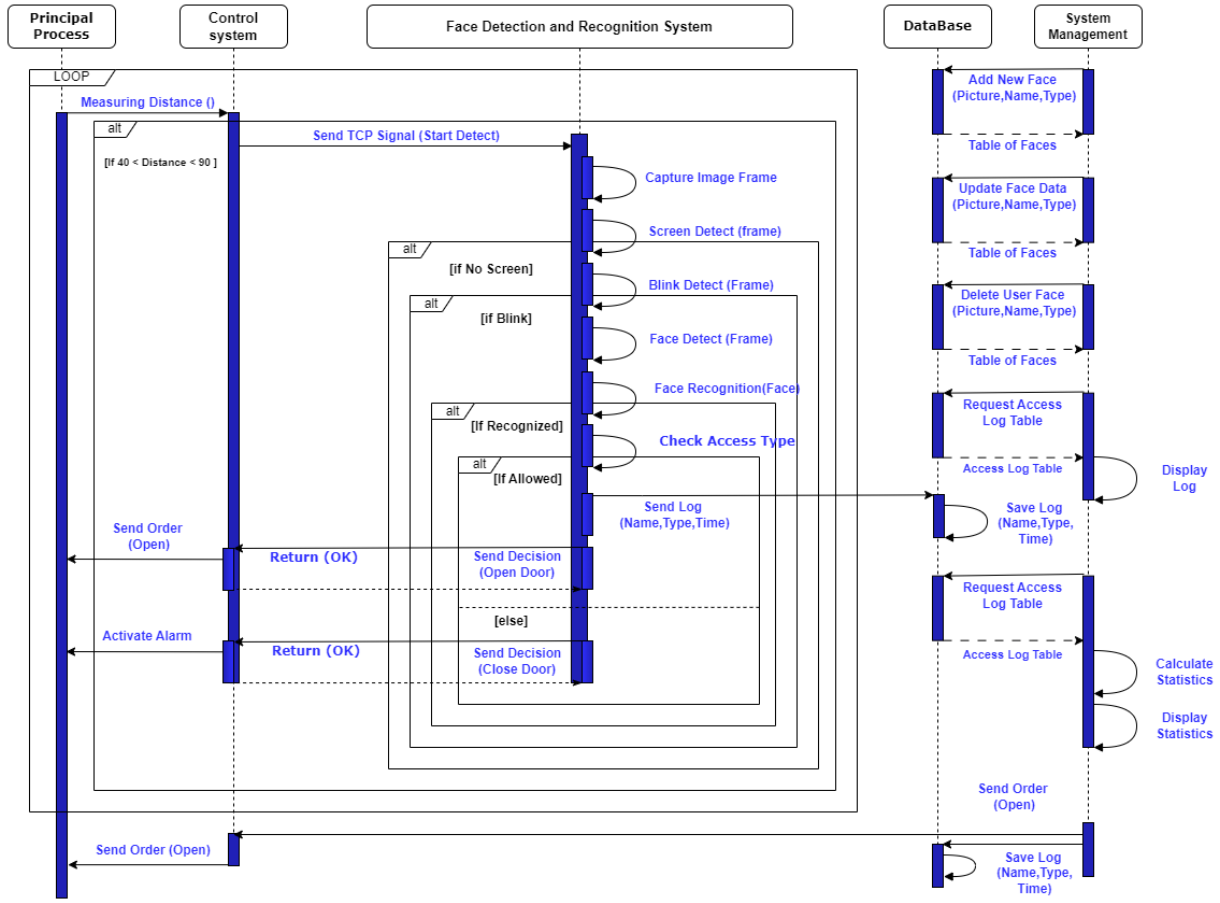

Figure 4.5: UML Sequence Diagram of VeriFace Gate System

1. The user approaches the door and enters the camera zone.
2. The Raspberry Pi checks if the user is within the valid distance range (40 - 90 cm).
3. If the distance condition is satisfied, the Raspberry Pi sends a TCP signal to the server to start the detection process.
4. The camera captures a frame of the users face.
5. The captured image is analyzed by YOLOv8s to detect if it is a spoof attempt (e.g., phone or screen).
    - **If spoofed:** detection is stopped, an alert is sent to the owners email, and access is denied.
6. If the input is genuine, the system proceeds to perform liveness detection using Dlib (blink detection).
    - If no blink is detected: access is denied and an alert is sent.
7. If a blink is detected: the face is located using MTCNN.

8. The face is encoded into an embedding using FaceNet.
9. The generated embedding is compared to the records in the MySQL database.
    - **If no match is found:** access is denied.
10. If a match is found: the system checks the access permission (Allowed or Denied).
    - **If Denied:** Sends an email alert to the owner
    - **If Allowed:** the server sends a command to Raspberry Pi to unlock the electronic lock.

4.2.2 Hardware part

The system relies on the following hardware components:

- **Raspberry Pi 5:** Acts as the central controller that manages signals, communicates with the server, and controls the lock.

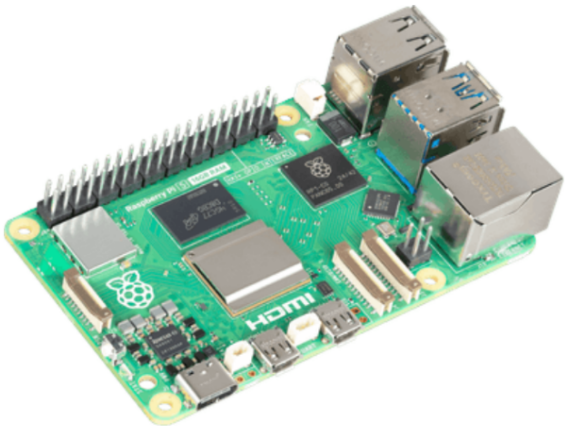

Figure 4.6: Raspberry Pi 5 [113]

- **Electronic Solenoid Lock:** Controls physical access by locking or unlocking the door.

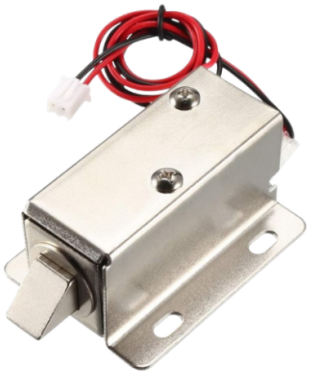

Figure 4.7: Electronic Solenoid Lock [99]

- **Breadboard:** Used for prototyping and connecting electronic components without soldering.

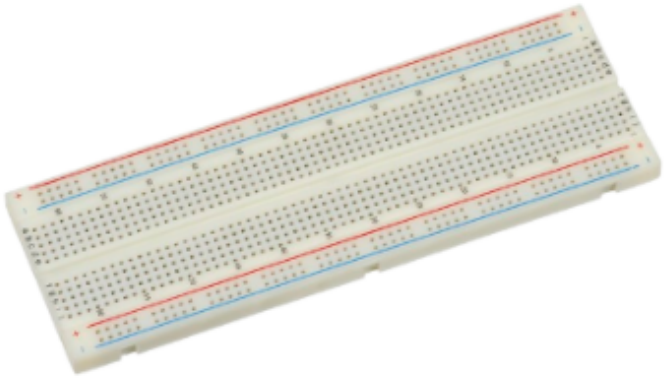

Figure 4.8: Breadboard [100]

- **LCD 16x2 Display:**Displays short text messages such as access status or system feedback.

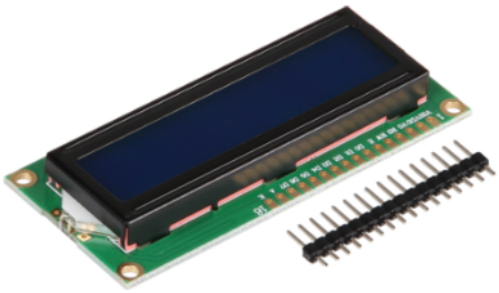

Figure 4.9: LCD 16x2 Display [101]

- **Ultrasonic Sensor:** Measures the distance of the person from the system to determine if recognition should start.

Figure 4.10: Ultrasonic Sensor [102]

- **LEDs:**Provide visual indicators for system status (access granted,denied,in progress)

Figure 4.11: LEDs [103]

- **Buzzer:** Emits sound alerts based on access results or system warnings.

Figure 4.12: Buzzer [104]

- **Relay Module:** Acts as a switch to control the power to the solenoid lock.

Figure 4.13: Relay module [105]

- **Camera:** Captures video feed for face detection and recognition.
- **3D case:** protects and houses the internal components.

4.2.2.1 Hardware architecture

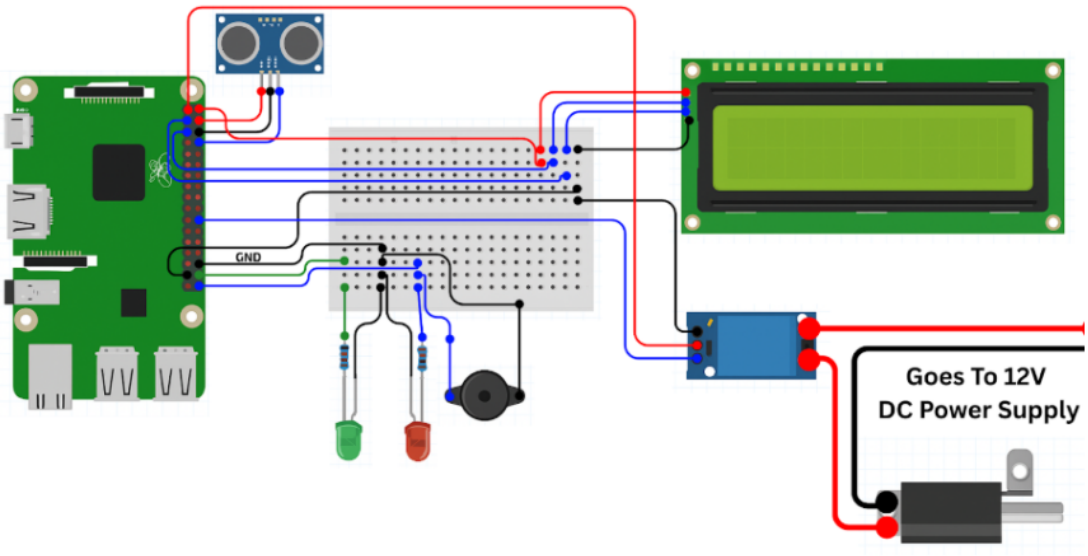

Figure 4.14: Hardware system design

To illustrate how these components are wired, the following circuit diagram in Figure 4.14 was created using the "Fritzing" software https://fritzing.org/ that provides a visual representation of the electrical layout of the system.

Heres the description detailing how the components are connected:

- The VCC of the LCD is connected to 3.3V of the Rasspbery.
- The GND of LCD is connected to the GND on the BreadBoard.
- The SDA (I2C serial data pin) of LCD is connected to the GPIO of Rasspbery.
- The SCL (I2C serial clock pin) of LCD is connected to the GPIO of Rasspbery.
- The VCC of the UltraSonic is connected to 5V of the Rasspbery.
- The GND of UltraSonic is connected to the GND on the BreadBoard.
- The Echo of UltraSonic is connected to the GPIO of Rasspbery.
- The Trigger of UltraSonic is connected to the GPIO of Rasspbery.
- The LED Green is connected to the GPIO of Rasspbery.
- The LED RED is connected to the GPIO of Rasspbery.
- The Buzzer is connected to the GPIO of Rasspbery.
- The Relay Singal is connected to the GPIO of Rasspbery.
- The Relay GND is connected to the Rasspbery

- The Relay VCC connected to the 5V of Rasspbery
- The Lock Solenoid - 12V connected to the Alimentation Power

4.2.3 Software Part

4.2.3.1 Dataset Base

The system uses a MySQL database named **face_recognition_db** to manage authentication, user data, and access logs. It consists of three main tables:

- **users:** Stores administrator credentials with hashed passwords to ensure secure login to the web interface.
- **known_faces:** Contains the names and facial image data (stored as BLOBs) of all individuals recognized by the system, along with their access status (Permission or Forbidden).
- **access_log:** Records every access attempt, including the person's name, timestamp of the event, and the type of access (e.g., granted or denied).
- This database structure supports real-time recognition, access control, and system monitoring through the web dashboard.

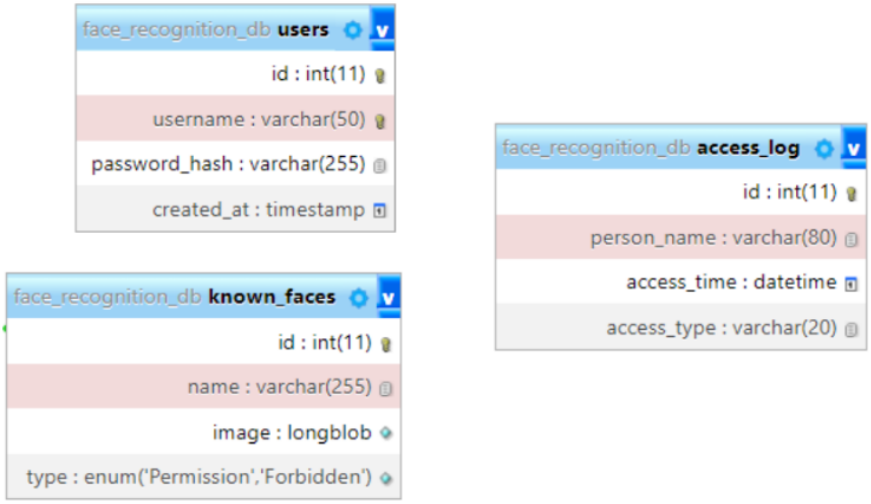

Figure 4.15: Architucte of Database

4.2.3.2 Data Real-Time Storage

All data processing related to face recognition and detection within our system occurs locally on a server. The result of each recognition attempt the individual's name, access time, and access permission (granted or not granted) is being stored in real time into a MySQL database. There are tables within this database that are structured to manage users, recognized faces, and access logs. The **access_log** table stores indepth event history, and the

known_faces table stores facial information and access type (Permission or Forbidden).web interface using Flask is used to interact with the system, such that administrators can see logs in real time, manage user access, monitor live camera feeds, remotely open or close the door, and receive images of unauthorized access attempts via email.

This local setup provides secure and efficient storage and management independent of cloud systems, providing a unique and reactive system.

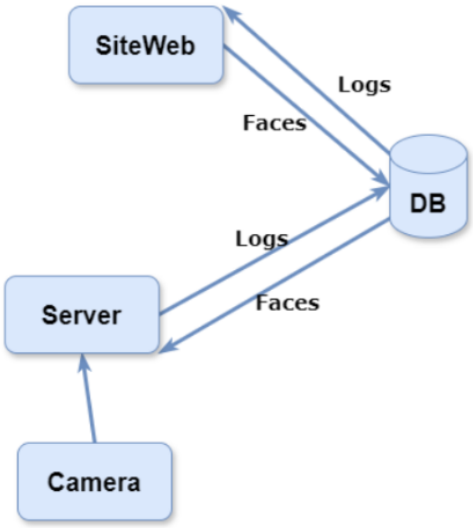

Figure 4.16: Data Real Time Storage

4.2.3.3 Face Detect Using Machine Learning Models

Face detection is a critical initial step in any facial recognition system. It consists of identifying and localizing human faces within an image or video stream. In our access control project, we leverage Transfer Learning to build an efficient and accurate face detection module without need to train a model from scratch.

We adopted the MTCNN (Multitask Cascaded Convolutional Networks) architecture, which is a well known deep learning model pretrained on large facial datasets. By using transfer learning, we benefit from the rich learned features of this model such as facial symmetry, eye alignment, and contour boundaries which allow it to perform robustly even in complex environments with varying lighting conditions, head poses, and occlusions. The model operates in three cascaded stages:

- **P-Net (Proposal Network):** Generates candidate facial regions.
- **R-Net (Refinement Network):** Refines these candidates by eliminating false positives.
- **O-Net (Output Network):** Detects facial landmarks (eyes, nose, mouth) with precision.

Rather than training the model entirely on our own dataset which would require hundreds of labeled images and significant computationwe fine tuned the model using a small

set of local face images captured from our camera setup. This process allowed the model to adapt to the specific visual context and resolution of our system, improving detection accuracy and reducing false positives in real world use.

Moreover, we integrated a distance sensor to activate the detection process only when a person is within an optimal range (typically 40 to 90 cm), minimizing unnecessary computations and improving the speed of the system. The Raspberry Pi detects the presence and sends a trigger to the server, which then activates the face detection pipeline.

4.2.3.4 Face Detect Prediction Using deep Learning Models

Face recognition is the core functionality in our intelligent access control system. Once a face is detected, the system must determine the identity of the individual by comparing it to a database of known users. Given the challenges of training deep face recognition models from scratchincluding data availability, computational cost, and time Transfer Learning emerges as the ideal solution.

We implemented face recognition using the FaceNet architecture, a powerful deep learning model trained on millions of facial images. FaceNet does not classify identities directly. Instead, it extracts a face embedding a 128 dimensional vector representing the unique features of a face. The closer two embeddings are in vector space, the more similar the two faces are.

Using Transfer Learning, we reused the pretrained FaceNet model and finetuned it on a small, local dataset of authorized users captured via our system. This allowed the model to adapt to the specific lighting, camera angle, and image resolution used in our environment, improving the accuracy of recognition without requiring a large dataset.

The recognition process follows these steps:

- A face is detected and cropped from the camera feed.
- The cropped image is passed to the FaceNet model to generate an embedding.
- This embedding is compared to all stored embeddings in the database using a distance metric.
- If the smallest distance is below a certain threshold, the face is considered a match; otherwise, access is denied.

A key refinement in our system was adjusting the threshold value. During testing, it was observed that individuals with similar facial features (such as siblings) could sometimes be confused. By lowering the threshold, we reduced the systems tolerance for similarity, which helped minimize false acceptances.

This Transfer Learning approach to face recognition ensures:

- High accuracy, even with limited data.
- Rapid deployment, since training from scratch is avoided.

- Efficient storage, since only compact embeddings are saved.
- Scalability, allowing new users to be enrolled by simply capturing their image and generating an embedding.

The combination of FaceNets precision, Transfer Learnings adaptability, and embedding based matching forms the intelligent and flexible recognition engine behind our secure access control system.

4.2.3.5 Anti Spoofing Techniques Using YOLO and Blink Detection

In biometric based security systems, especially those relying on facial recognition, spoofing attacks represent a significant threat to the reliability and safety of access control. Spoofing occurs when an unauthorized individual attempts to deceive the system by presenting a photograph, video recording, or screen display of a legitimate user. To counter these threats and ensure the authenticity of the presented face.

the proposed system integrates two advanced anti spoofing mechanisms:
object detection using the YOLOv8s model a
Eye blink detection using a deep learning approach.

The first layer of defense leverages the YOLO (You Only Look Once) object detection model, which was trained to recognize various devices such as phones, tablets, and monitors. When a face is detected, the YOLO model scans the surroundings of the face to identify if any of these devices are visible. If a screen or phone is detected in the frame, it strongly suggests that the face might be coming from a digital device rather than a real person. In such cases, the system immediately halts the recognition process and classifies the attempt as suspicious, effectively preventing unauthorized access based on artificial presentations.

However, detecting devices alone is not sufficient to eliminate all spoofing risks, especially in cases where the attacker uses printed photos or 3D masks. To enhance the robustness of the system, a second layer of verification is added in the form of blink detection, which ensures liveness of the individual. This mechanism is based on analyzing a short video sequence of the face to monitor eye movement. A convolutional neural network (CNN) model processes the eye region to detect whether a natural blinking pattern is present within a predefined time window. The absence of a blink or the presence of unnatural eye behavior is a strong indicator of spoofing, prompting the system to reject the attempt.

By combining these two techniques YOLO based screen detection and CNN based blink detection the system achieves a higher level of security and ensures that only live, physically present individuals are granted access. This dual layered approach strengthens the defense against common attack vectors and improves the reliability of the face recognition component in real world scenarios, especially in sensitive environments such as restricted areas, laboratories, or corporate facilities.

4.2.3.6 Distance Verification Using an Ultrasonic Sensor

In addition to visual and behavioral verification techniques, physical proximity plays a crucial role in ensuring the reliability and authenticity of users in biometric access control systems. One of the challenges faced by facial recognition systems is distinguishing between legitimate users standing at an appropriate distance from the camera and spoofing attempts using distant screens or printed photos. To address this issue, our system incorporates an ultrasonic distance sensor as an additional layer of verification, ensuring that face recognition is only performed when the subject is within a predefined range from the camera.

The ultrasonic sensor operates by emitting a sound wave and measuring the time it takes for the echo to return after hitting an object. Using this time difference, the system calculates the exact distance between the camera and the subject. In our implementation, the system is configured to only proceed with face recognition if the detected person is located between 40 cm and 90 cm from the camera. This range was determined experimentally to offer a balance between facial clarity for recognition purposes and rejection of potential spoofing attempts from distant devices.

By enforcing this distance constraint, the system effectively prevents common spoofing techniques such as presenting a large screen from afar or holding a printed image at an angle. If the person is too close or too far, the system automatically disables the face detection module and notifies the user to adjust their position. This not only improves recognition accuracy but also ensures that the system is interacting with a real individual physically present in front of the device.

Moreover, this sensor-based approach operates in real time and adds minimal latency to the system, making it suitable for access control scenarios that require both speed and security. Combined with blink detection and screen identification using YOLO, the distance verification acts as a third barrier against spoofing, reinforcing the overall trustworthiness of the biometric security framework.

This method demonstrates how the integration of hardware components like the ultrasonic sensor can complement AI based models, resulting in a hybrid system that is both intelligent and context aware, capable of adapting to real world constraints and threats.

4.2.3.7 Performance Evaluation Metrics

In order to assess the performance of the proposed artificial intelligence models, a set of **standard evaluation metrics** was employed. These metrics provide an objective and quantitative way to measure how well the models perform on classification tasks. The following four metrics were selected for their ability to represent different aspects of model effectiveness: Accuracy,**Precision**,**Recall**, and **F1-Score**.

1. Accuracy :

Accuracy is the most intuitive performance measure, representing the ratio of correctly predicted instances (both true positives and true negatives) to the total number of predictions.

It answers the basic question: "How often is the classifier correct?

$$\frac{TP + TN}{TP + TN + FP + FN} = Accuracy \tag{4.1}$$

TP: True Positives correctly identified positive cases
TN: True Negatives correctly identified negative cases
FP: False Positives negative cases incorrectly classified as positive
FN: False Negatives positive cases incorrectly classified as negative

2. Precision :
Precision evaluates the models ability to provide relevant results. It is defined as the proportion of positive identifications that were actually correct. It is especially important in applications where false positives are costly.

$$\frac{TP}{TP + FP} = Precision \tag{4.2}$$

3. Recall (Sensitivity):
Recall measures the models ability to detect all actual positive instances. It is crucial when the cost of missing a positive instance (false negative) is high. This metric answers the question: "How many actual positives were captured by the model?"

$$\frac{TP}{TP + FN} = Recall \tag{4.3}$$

4. F1-Score :
The F1-Score is the harmonic mean of precision and recall. It provides a balanced measure when one seeks to maximize both precision and recall simultaneously. This is especially useful in imbalanced datasets, where accuracy can be misleading.

$$\frac{Precision \times Recall}{Precision + Recall} = F1 - Score \tag{4.4}$$

These four metrics were adopted as the cornerstone for evaluating the detection and recognition components of the system, providing a comprehensive overview of performance across different AI modules.

4.2.4 The 3D Design

The 3D model of our wearable device consists of a case 4.17,4.18,4.19,4.20, which designed in Site ' tinkercad ' and printed it in University
The 3D cases design.

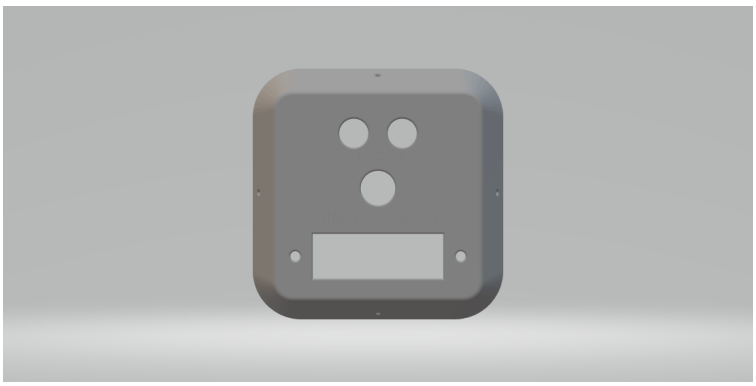

Figure 4.17: Outside Case

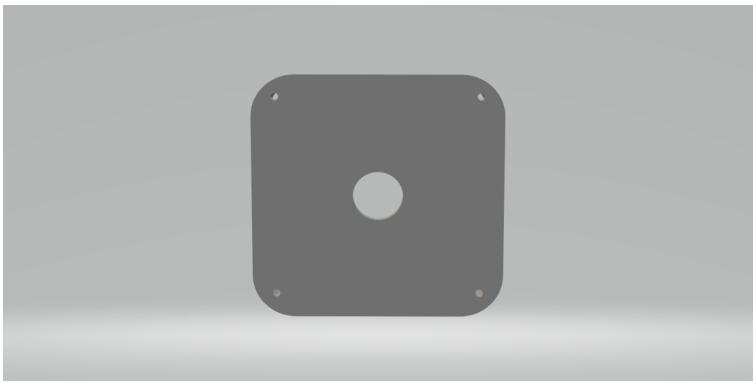

Figure 4.18: Outside Base Case

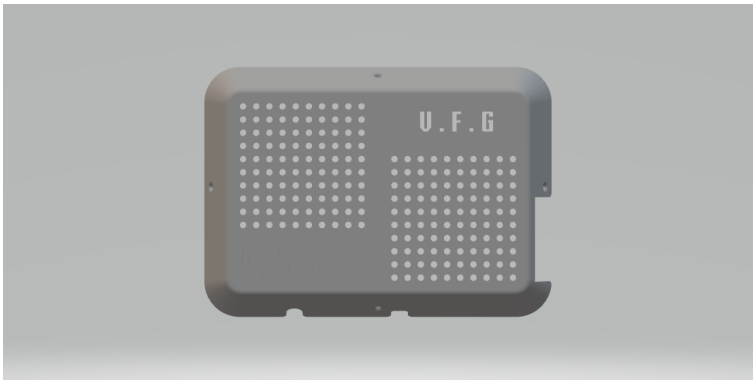

Figure 4.19: Inside Case

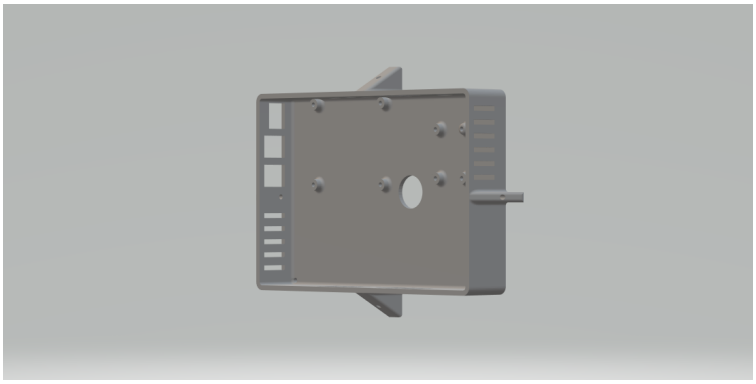

Figure 4.20: Inside Base Case

4.3 Implementation

In this section, the focus will be on the practical aspects of the project. We will begin by introducing the tools we have used, including both software and hardware. Well then present the hardware implementation and the software development.

4.3.1 Languages and tools for development

We will cover the tools and platforms we have used starting by hardware tools and then moving on to software tools.

4.3.1.1 Hardware tools

The development and testing of the system were carried out using two different laptops, each with distinct hardware configurations, in order to ensure compatibility and performance stability across various environments.

The first machine used was an HP EliteBook, equipped with an Intel®Core™ i7-5600U processor, 12 GB of DDR3 RAM, and Intel HD Graphics 5500, running on Windows 10. This setup provided a stable environment for development and initial testing.

The second device was an ASUS Pro laptop featuring a 10th Generation Intel® Core™i3-10110U processor, 20 GB of DDR4 RAM, and operating on Windows 11. This configuration allowed us to test the system under a more modern OS and higher memory capacity, ensuring efficient performance, especially during multitasking and resource-intensive processes.

Using both machines helped validate the system's responsiveness, adaptability, and overall functionality in different hardware and software contexts

Anycubic i3 Mega 3D printer: is a user-friendly
3D printer with a build volume suitable for most hobbyist projects. Inspired by the Prusa i3 design, it offers a maximum print size of 210 x 210 x 205 mm. While not the largest print area, it allows for creating a variety of objects. The printer can achieve fine resolution down to 50 microns, ensuring detailed prints.[119].

Figure 4.21: Anycubic i3 Mega 3D printer logo [119]

TigerVNC TigerVNC is a high-performance, platform-neutral implementation of VNC (Virtual Network Computing), a client/server application that allows users to launch and interact with graphical applications on remote machines. TigerVNC provides the levels of performance necessary to run 3D and video applications, and it attempts to maintain a common look and feel and re-use components, where possible, across the various platforms that it supports. TigerVNC also provides extensions for advanced authentication methods and TLS encryption.[121]

Figure 4.22: tigerVNC Viewer logo [121]

4.3.1.2 Software tools

- **Visual Studio** as an integrated development environment (IDE) from Microsoft used for developing applications in various programming languages.

Figure 4.23: Visual Studio logo [106]

- **Python** programming language known for its readability and wide range of applicatio

Figure 4.24: Python logo [107]

- **Flask** A high-level Python web framework that encourages rapid development and clean, pragmatic design

Figure 4.25: Flask logo [[108]

- **Tinkercad** An online 3D modeling and circuit simulation tool used for designing and visualizing electronic circuits and creating 3D digital designs

Figure 4.26: Tinkercad logo [109]

- **HTML** The standard markup language used for creating and structuring content on the web

Figure 4.27: HTML logo [110]

- **CSS** A style sheet language used for describing the presentation of a document written in HTML or XML

Figure 4.28: CSS logo [111]

- **JavaScript (JS)** is a lightweight, interpreted programming language used to create dynamic and interactive behavior on websites

Figure 4.29: JavaScript (JS) logo [112]

- **Fritzing:** An open-source software tool for designing and prototyping electronics projects by creating schematics and PCB layouts [120]

Figure 4.30: Fritzing logo [120]

- **XAMPP** : is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use.[122]

Figure 4.31: XAMPP Control Panel logo [122]

4.3.2 Hardware Realisation

After using "Fritzing" software for modeling our device circuit, we connect the components together accordinly by following the connections shown in the softwares circuit diagram Figure 4.14. Following the connections shown in the Fritzing softwares circuit diagram ensures that all components are properly linked and can function as intended. The software "Fritzing" is a well liked tool for designing circuit diagrams and PCB layouts, providing a visual representation of the circuits parts and connections. The physical result of the hardware connection explained above is illustrated in Figure 3.28. This prototype offers a clear and complete picture of the finished circuit by displaying the real components and their connections.

Figure 4.32: Material en real

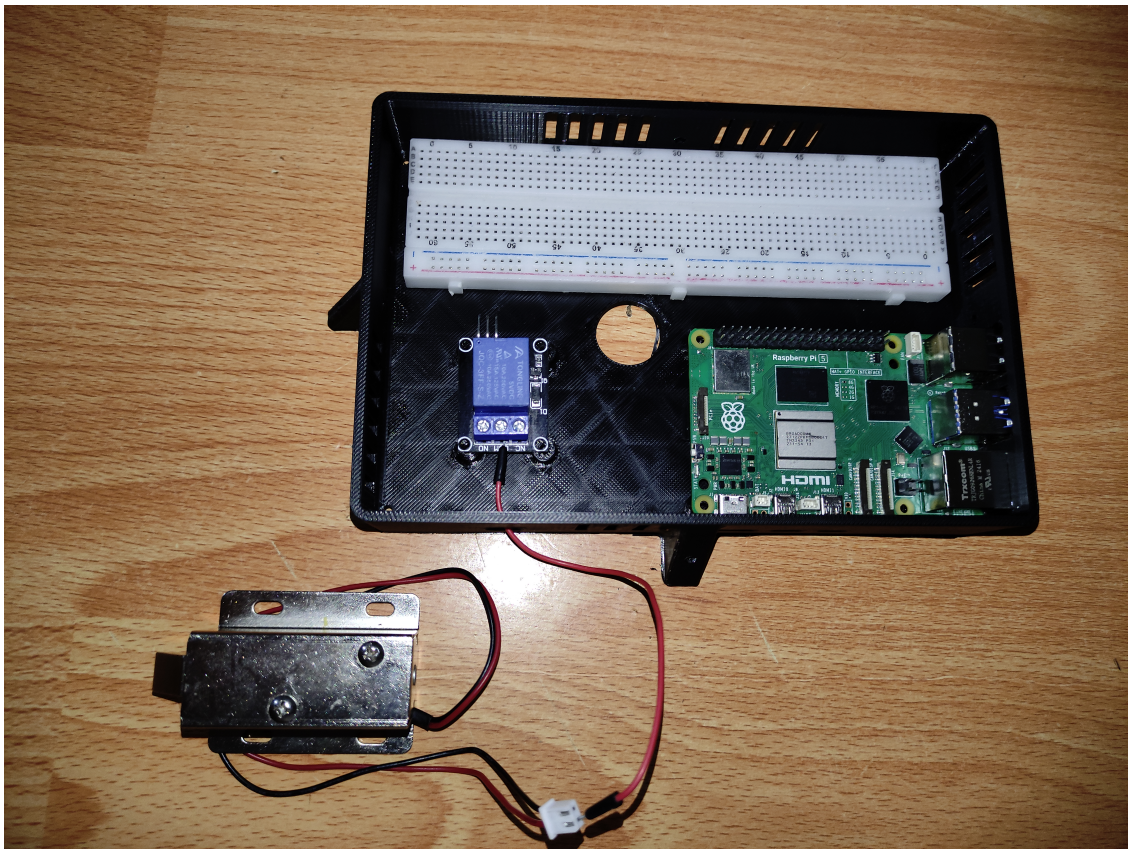

Figure 4.33: Material en real 2

4.3.3 Software Realisation

4.3.3.1 Implementation Of YMF-TL model

The implementation of **YMF-TL** (YOLO,MTCNN and FACENET Using Transfer Learning) model in our access control system forms the backbone of its intelligent decision-making capabilities. The core AI components consist primarily of face detection, face recognition, liveness detection, and spoofing preventionall integrated into a unified pipeline that ensures both speed and reliability in real-time scenarios. These models were carefully chosen and adapted to function efficiently within the constraints of the system's hardware and operational requirements.

For face detection, the system employs the MTCNN (Multi-task Cascaded Convolutional Networks) model, which offers high accuracy and robustness in locating facial landmarks even under varying lighting conditions or angles. This model is responsible for identifying the presence of a face in the video stream and cropping it for further analysis. Once a face is detected, it is passed to the FaceNet model for embedding extraction. FaceNet generates a 128-dimensional feature vector representing the unique characteristics of the individuals face, which is then compared against a stored database using cosine similarity or Euclidean distance to determine identity.

To improve efficiency and reduce training costs, the system adopts Transfer Learning, wherein pre-trained models on large datasets are fine-tuned using a smaller set of local user images. This not only reduces the computational requirements but also allows rapid deployment in new environments with minimal data collection.

Additionally, the system incorporates YOLOv8s, a lightweight but powerful object detection model, to recognize the presence of devices such as phones or screens that may indicate spoofing attempts. This model was trained using a custom dataset that includes various scenarios , enabling the system to react intelligently to visual context.

Complementing the visual models is the eye-blink detection module, implemented using a Convolutional Neural Network (CNN) trained to classify eye states (open/closed) over a short temporal window. This allows the system to assess liveness, rejecting inputs that lack natural eye movement.

The YMF-TL model are executed on the central server rather than on the Raspberry Pi to ensure smooth performance. The Raspberry Pi acts as an IoT edge device that captures signals (e.g., distance or button press) and relays them to the server to trigger the AI processing pipeline. Once a decision is made (authorized/denied), a signal is sent back to the Pi to control the electronic lock.

Our model a modular implementation demonstrates the power of AI in real-time biometric access systems, combining accuracy, security, and hardware integration to provide a seamless and tamper-resistant experience.

4.3.3.2 The Website

In order to bring the facial recognition access control system components together in its entirety, we designed a web interface via the Flask framework.

This interface serves as the system control panel for all system operations, in which the administrator is able to observe the live camera display, open or close the door remotely, and monitor access attempt records and examine associated statistics.Data is transmitted from the server to the site in real time using secure protocols. Data transmitted includes that of the identified person, attempt time, and permission or denial status.It has database management (adding, changing, or deleting faces), genuine system activity tracking, and also email notification or images if suspicious strangers are identified.

This seamless integration between artificial intelligence, physical system, and web interface gives a complete and streamlined user experience in a secure environment.

- **The login page** is the secure gateway to the website. The user is required to enter their credentials to access the administrative interface.

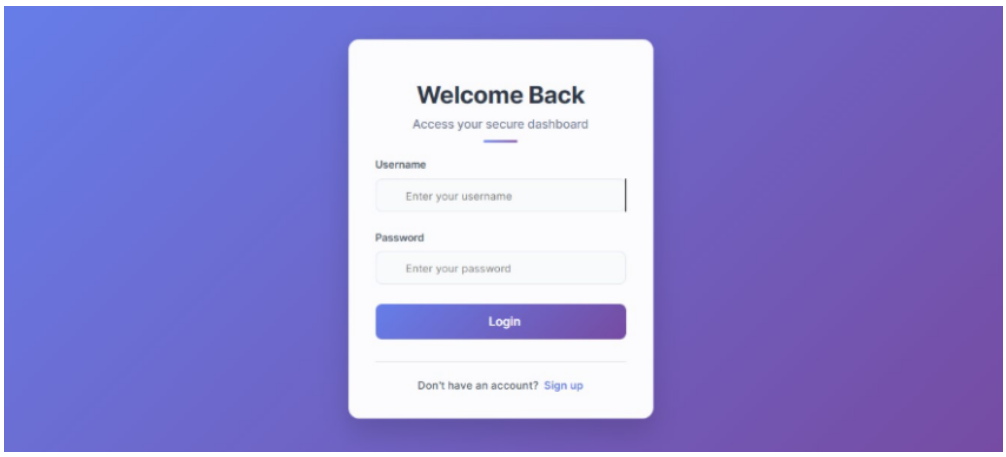

Figure 4.34: The login page

- **Sign up page** Used to add new accounts for administrators or authorized users, specifying their permissions within the system.

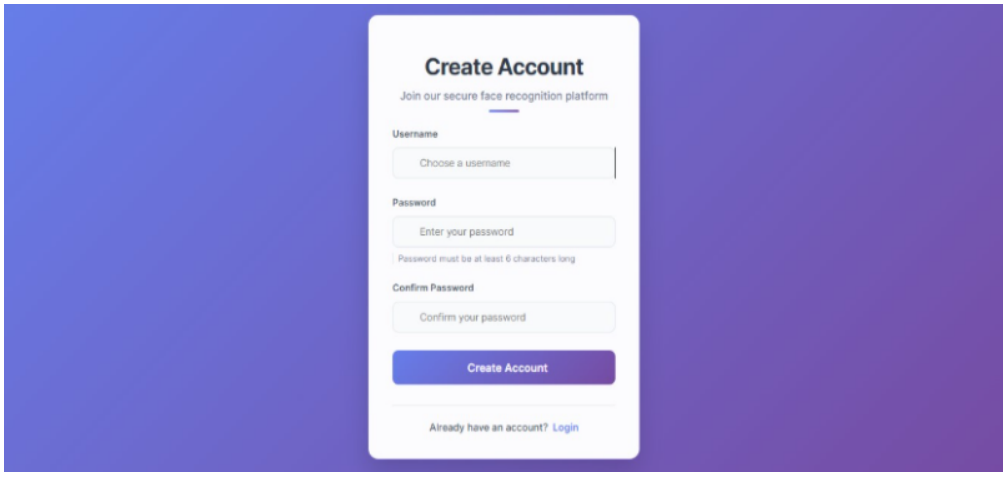

Figure 4.35: Sign up page

- **The home page (Dashboard)** Represents the system's general interface. It displays all site pages and enables the administrator to monitor the live camera feed, allowing them to monitor the perimeter of the entry point and make quick decisions in the event of any unusual activity.

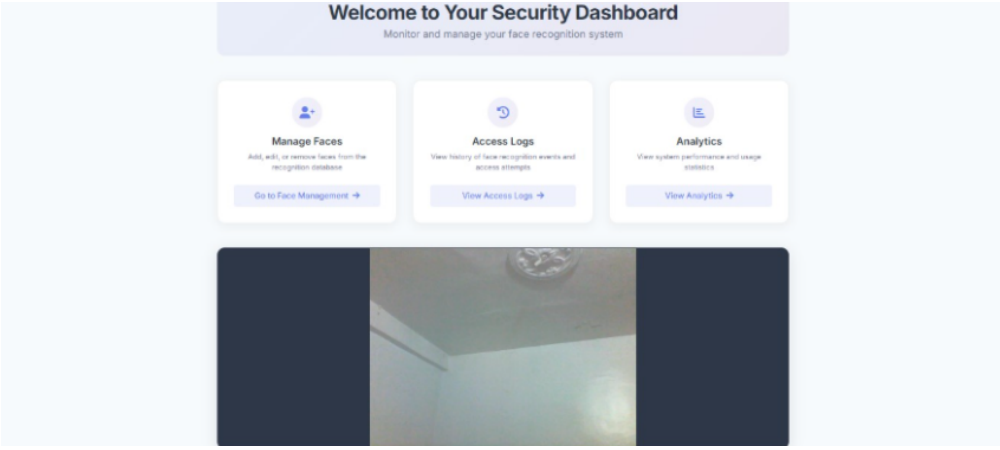

Figure 4.36: The home page

- **The Face Management page** is used to manage the face database by adding, modifying, or deleting users, with precise access permissions for each person.

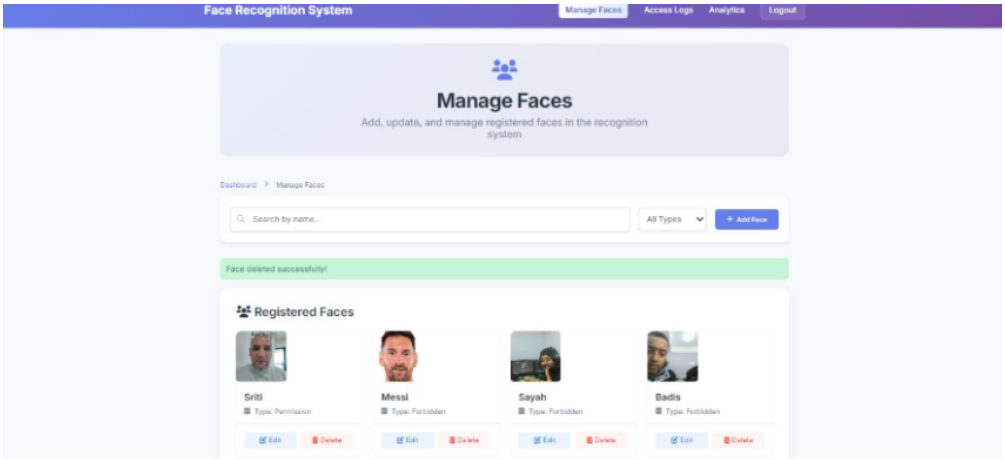

Figure 4.37: The Face Management page1

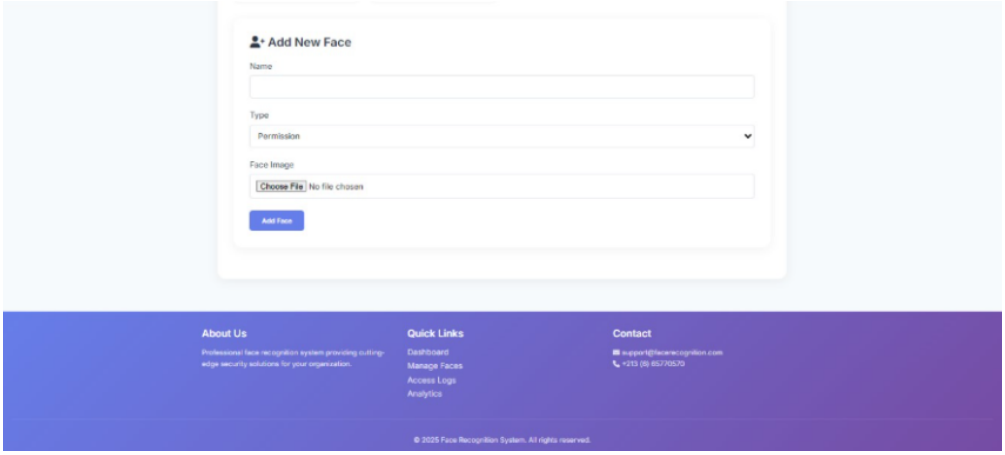

Figure 4.38: The Face Management page2

- **The Logs page** provides a detailed chronological record of all login attempts, including the user's details, the time of the attempt, the permission or denial status, and the capture image.

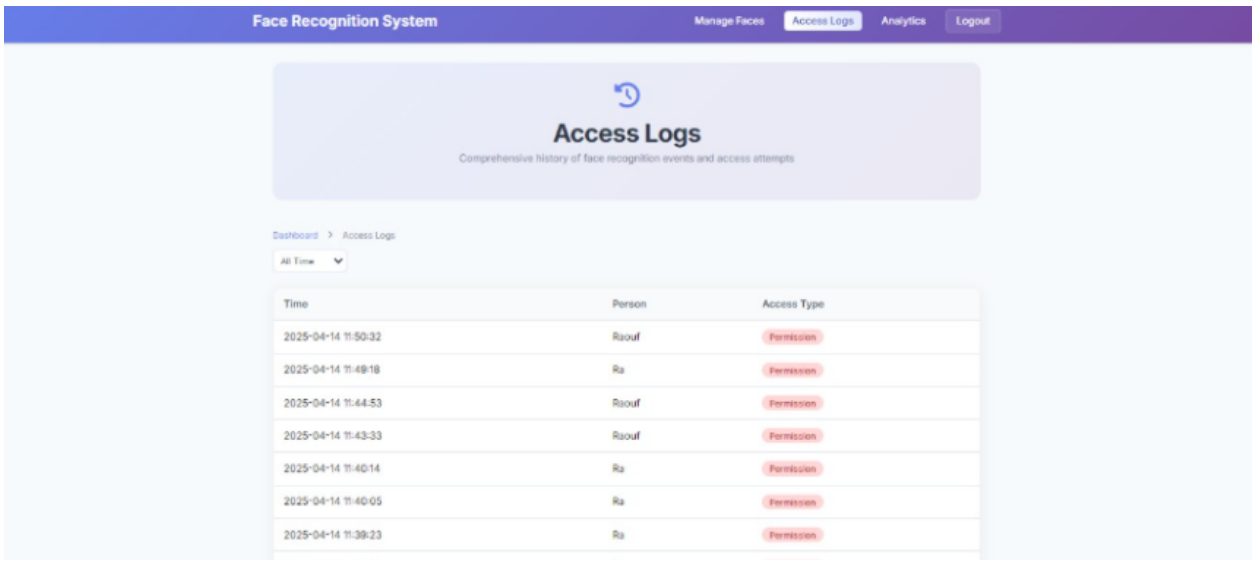

Figure 4.39: The Logs page

- **The Statistics page** displays graphs and quantitative analysis that help understand system behavior over time and identify peak times or suspicious activity.

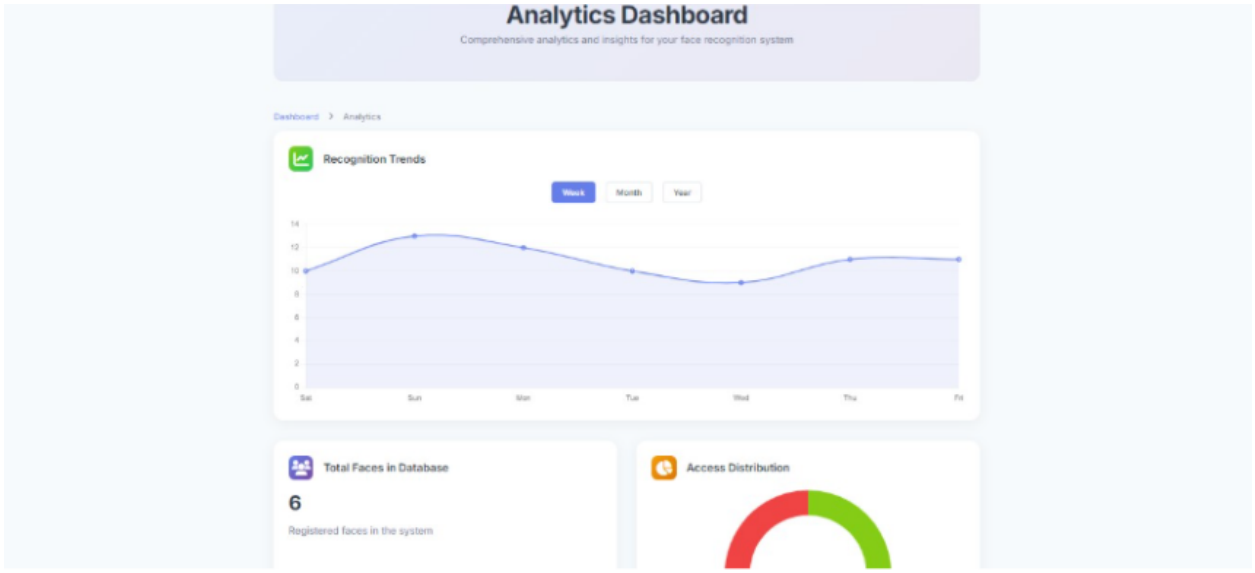

Figure 4.40: The Statistics page

- **The Lock Control page** enables the administrator to open or close the electronic lock remotely. All transactions are recorded for tracking and transparency purposes.

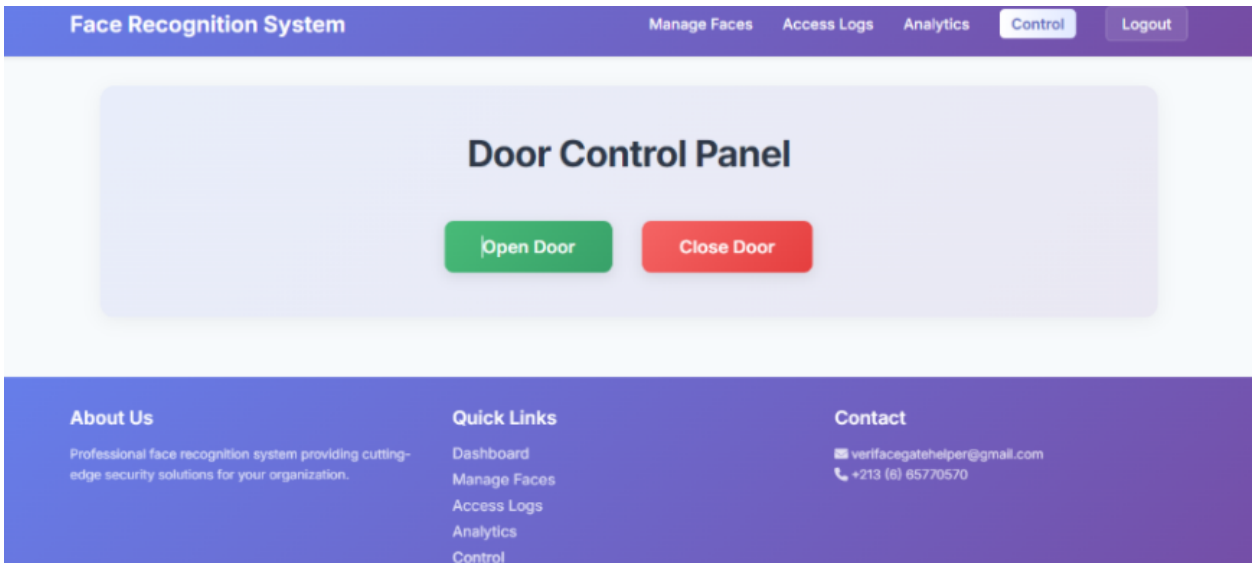

Figure 4.41: The Lock Control page

4.3.4 Prototype Realisation

4.3.4.1 3DModel Printing

Figure 4.42: 3DModel Printing 1

Figure 4.43: 3DModel Printing 2

4.4 Conclusion

In this chapter, we provide a complete description of the design and development of the suggested facial recognition-based smart access control system. We first describe the composition of the system as a whole, which consists of hardware components such as the camera and Raspberry Pi, and software components such as the artificial intelligence algorithms and web interface.

The development tools and environment used are explained, along with the specific steps executed to integrate the various system elements. We discuss practical matters pertaining to the face detection feature, data management, database connectivity, and permission management through the interactive interface.In the next chapter, we present details regarding the experiments carried out to check the performance of the system and then the comparison of the results obtained from hardware and software aspects. We contrast these results with previous work in order to highlight the strengths and advantages of the proposed system.

Chapter 5

Experimentation results and Discussion

5.1 Introduction

Evaluating the performance of each subsystem within an access control solution is essential to ensure reliability, robustness, and security. In this chapter, we present a comprehensive experimental evaluation of the two core components of our system: the face verification module (based on MTCNN for detection and FaceNet with Inception ResNet V1 for feature extraction) and the spoof prevention module (based on YOLOv8s for detecting electronic devices such as phones and screens). Each module was evaluated independently on separate datasets specifically constructed to simulate real-world usage scenarios.

The face verification component was tested on a large dataset comprising 5000 face images, measuring its capability to distinguish between identities with high accuracy using cosine distance metrics. Similarly, the YOLOv8s object detection model was evaluated on over 9500 images, including both images containing screens and images without, to validate its efficiency in detecting spoofing attempts via electronic displays.

This chapter details the experimental methodology, dataset preparation, and performance metrics used, including Accuracy, Precision, Recall, F1-Score, and Receiver Operating Characteristic (ROC) Curves. We also provide insights into true/false positives and negatives, and discuss the implications of the results on the systems real-world deployment and trustworthiness. These experiments not only provide insights into the strengths and limitations of each component but also demonstrate the overall reliability of the system in realistic scenarios involving both identity verification and spoofing prevention.

5.2 Results of AI algorithms

This section presents the evaluation and analysis of the core artificial intelligence components integrated into the proposed access control system. Each algorithm was tested individually to ensure its effectiveness, robustness, and contribution to the overall reliability and security of the system.The tested modules include:

- A mobile screen detection system, designed to detect the presence of phone or screen images before the facial verification process.
- A face detection system, responsible for identifying,extracting faces from input images.
- A face recognition system, which verifies the identity of individuals by comparing facial embeddings against a reference database.

The following subsections describe the testing methodology, data preparation process, result calculation, and analysis for each of these AI components.

5.2.1 Testing Mobile Screen Detection System

This section focuses on evaluating the performance of the mobile screen detection system, which is used to enhance the robustness of the overall face recognition architecture by rejecting spoofing attempts involving phone or screen images. The objective is to determine whether the system can reliably detect the presence of screens in an image before face recognition is initiated.

The evaluation is conducted using a pretrained YOLOv8s object detection model operating in a classification context. A custom dataset was assembled for this purpose, and the models performance was analyzed based on common classification metrics such as accuracy, precision, recall and F1-score.

The following subsections present the method used for testing, data preparation steps, detailed calculation of the results, and an in-depth analysis of the systems performance.

5.2.1.1 Testing Method

we conducted a large-scale test using a dataset composed of 9,266 images, carefully curated to simulate realistic and diverse environments. The dataset included images with a wide variety of contents, such as people, buildings, indoor and outdoor scenes, and critically, images both with and without electronic screens (phones, tablets, and monitors). Each image was labeled using a ground truth CSV file, in which: Each row corresponds to a single image filename,A binary label indicates whether the image contains at least one screen (1) or not (0).

The detection process relied on the YOLOv8s model, configured to recognize three screen-related classes with COCO IDs: 62, 63, and 67, representing TV monitors, laptops, and cellphones respectively. For each image, YOLOv8s was executed to identify the presence of any object belonging to one of these three classes. If at least one screen-related class was detected with a sufficient confidence level, the model classified the image as containing a screen. After running inference on the entire dataset, the predictions were matched against the ground truth labels to compute the following performance metrics:

- **True Positives (TP):** Images correctly identified as containing screens.
- **True Negatives (TN):** Images correctly identified as not containing screens.
- **False Positives (FP):** Images incorrectly predicted to contain screens.
- **False Negatives (FN):** Images incorrectly predicted to not contain screens.

Using these values, we **derived standard evaluation metrics**:

- **Accuracy**
- **Precision**
- **Recall**
- **F1-Score**

This evaluation provides a clear assessment of the screen detection modules performance, particularly in distinguishing valid camera input from potential spoofing attempts via phones or display devices.

5.2.1.2 Data Preparation

To evaluate the mobile screen detection system, a custom dataset was created by collecting two distinct categories of images from the public dataset Kaggle. The first category consisted of **2137** images that contained at least one mobile phone or screen visible within the frame. These images were carefully selected to ensure they represent various lighting conditions, orientations, and contexts where mobile screens may appear.

The second category comprised **7,129** images that did not include any visible screens. These images primarily featured indoor and outdoor scenes, architectural structures, landscapes, and other common real-world scenarios, ensuring the absence of screens or handheld devices. This provided a robust negative class for the detection model to distinguish against.

All images were named sequentially and consistently using numeric filenames (e.g., 0001.jpg, 0002.jpg, ..., 9266.jpg). This naming convention facilitated the creation of a corresponding CSV file used during evaluation. The CSV file included two columns: one for the image filename and the second for the ground truth label 1 indicating the presence of a mobile screen, and 0 indicating its absence.

This structured labeling enabled the testing phase to run in a classification context, where the model output could be compared directly to the ground truth. Notably, the YOLOv8s model used in this evaluation was not trained from scratch but utilized in a transfer learning setting, using pre-trained weights to perform screen detection on the custom dataset.

5.2.1.3 Calculating Results

To evaluate the performance of the mobile screen detection system, the following classification metrics were computed based on the confusion matrix results:

True Positives (TP): 2116

True Negatives (TN): 7117

False Positives (FP): 12

False Negatives (FN): 21

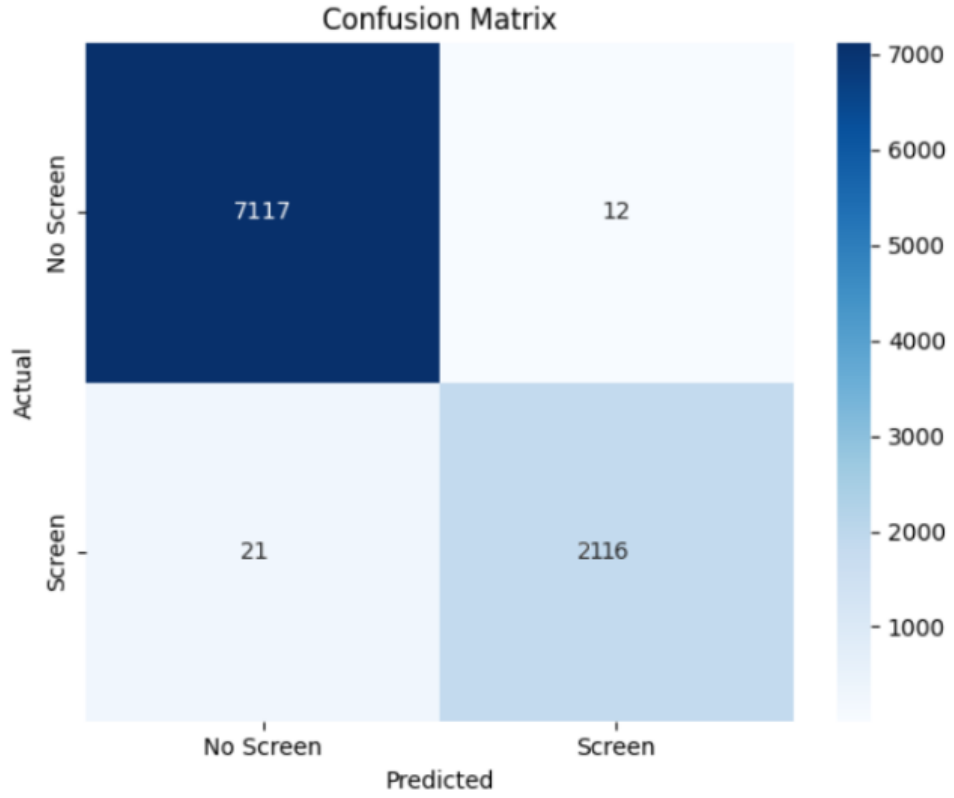

Figure 5.1: confusion matrix of Testing Mobile Screen Detection System

Using these values, the main evaluation metrics were calculated as follows:

- **Accuracy** measures proportion of correctly classified instances among all samples:

$$0.9964 \approx \frac{9233}{9266} = \frac{7117 + 2116}{21 + 12 + 7117 + 2116} = \frac{TP + TN}{TP + TN + FP + FN} = Accuracy$$

- **Precision** indicates the proportion of true positives among all predicted positives:

$$0.9944 \approx \frac{2116}{2128} = \frac{2116}{12 + 2116} = \frac{TP}{TP + FP} = Precision$$

- **Recall** measures the proportion of true positives detected among all actual positives

$$0.9902 \approx \frac{2116}{2137} = \frac{2116}{21 + 2116} = \frac{TP}{TP + FN} = Recall$$

- **F1-Score** is the harmonic mean of precision and recall:

$$0.9923 \approx \frac{0.9902 \times 0.9944}{0.9902 + 0.9944} \times 2 = \frac{Precision \times Recall}{Precision + Recall} \times 2 = F1 - Score$$

These metrics provide a numerical basis for assessing the systems detection accuracy and reliability. The interpretation of these results is discussed in the next section.

5.2.1.4 Analyzing Results

The performance results of the mobile screen detection system using the pretrained YOLOv8s model demonstrate a high level of accuracy and reliability in classifying images that contain mobile screens versus those that do not.

The accuracy of 99.64% indicates that the model correctly identified the presence or absence of screens in the vast majority of the 9266 test images. This suggests a strong generalization capability across diverse and challenging visual inputs.

The precision score of 99.44% shows that when the model predicts the presence of a screen, it is almost always correct. This is critical in security systems, where a false alarm (i.e., falsely detecting a screen when there is none) could disrupt the recognition process unnecessarily.

The recall of 99.02% highlights that the system is highly sensitive to the presence of screens, successfully identifying the vast majority of them. This means that very few actual screens went undetected, which is vital to ensuring spoofing attempts using phone or monitor images are reliably caught.

Finally, **The F1-score**, a balance between precision and recall, stood at **99.23%**, reinforcing the overall robustness and balance of the models performance.

In conclusion, the YOLOv8s model, when used as a classifier through transfer learning on unseen images, proves to be an effective and highly performant solution for mobile screen detection within the access control system. The few misclassifications (12 false positives and 21 false negatives) are minor relative to the size of the dataset and may be attributed to visual ambiguity or edge cases in the images.

5.2.2 Face Detection System Testing

This section presents the evaluation process of the face detection module integrated into our access control system. Accurate face detection is a foundational step in any biometric authentication pipeline, as it ensures that the system can correctly localize and extract faces from live video streams or still images before proceeding to recognition. The goal of this evaluation is to determine the precision, robustness, and limitations of the deployed detection algorithm under real-world conditions. The system under test is based on the MTCNN (Multi-task Cascaded Convolutional Network), a well-established deep learning model known for real-time face localization with high accuracy.

The following subsections will outline the testing methodology, the preparation of data used for evaluation, the metrics computed to quantify performance, and a detailed analysis of the observed results.

5.2.2.1 Testing Method

The face detection component plays a fundamental role in our biometric access control system. Its purpose is to accurately identify whether a face is present in a given image, serving as the first gate before proceeding to face recognition.
To evaluate this component, we employed a pretrained Multi-task Cascaded Convolutional Network (MTCNN), well known for its robustness and efficiency in real-world facial detection tasks.

The evaluation was performed using a dataset of 12,129 labeled images containing both face-present and face-absent scenarios. The detection model was applied to each image to determine whether at least one face was present. The output was then compared against the ground truth labels to classify the detection as either correct or incorrect. The comparison enabled the computation of standard classification performance metrics, including True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

The entire process was executed via a Python script, where the MTCNN model was used directly without retraining, following a transfer learning approach consistent throughout our project.

5.2.2.2 Data Preparation

The dataset used for testing the face detection system was constructed using publicly available image collections sourced from the Kaggle platform. It consisted of a total of 12,129 images, subdivided as follows:

- 5,000 images containing at least one human face, covering a wide range of facial poses, lighting conditions, and individual identities.
- 7,129 images containing no faces, primarily depicting urban, natural, and indoor environments such as buildings, roads, open spaces, and landscapes.

A ground truth file in CSV format was created to annotate the dataset. It included two columns: one for the image filenames and another indicating the presence (1) or absence (0) of a face in the respective image. This structured labeling enabled precise verification of the models predictions.

The naming of image files was done in a sequential manner to ensure consistency between the image paths and their corresponding ground truth labels. This made it easier to automate the evaluation pipeline and align results accurately with the reference annotations.

5.2.2.3 Calculating Results

To evaluate the performance of the face detection module, we computed standard classification metrics using the results obtained from the test dataset. Based on the predictions and the ground truth labels, the following values were recorded:

True Positives (TP): 4978
True Negatives (TN): 7092
False Positives (FP): 37
False Negatives (FN): 22

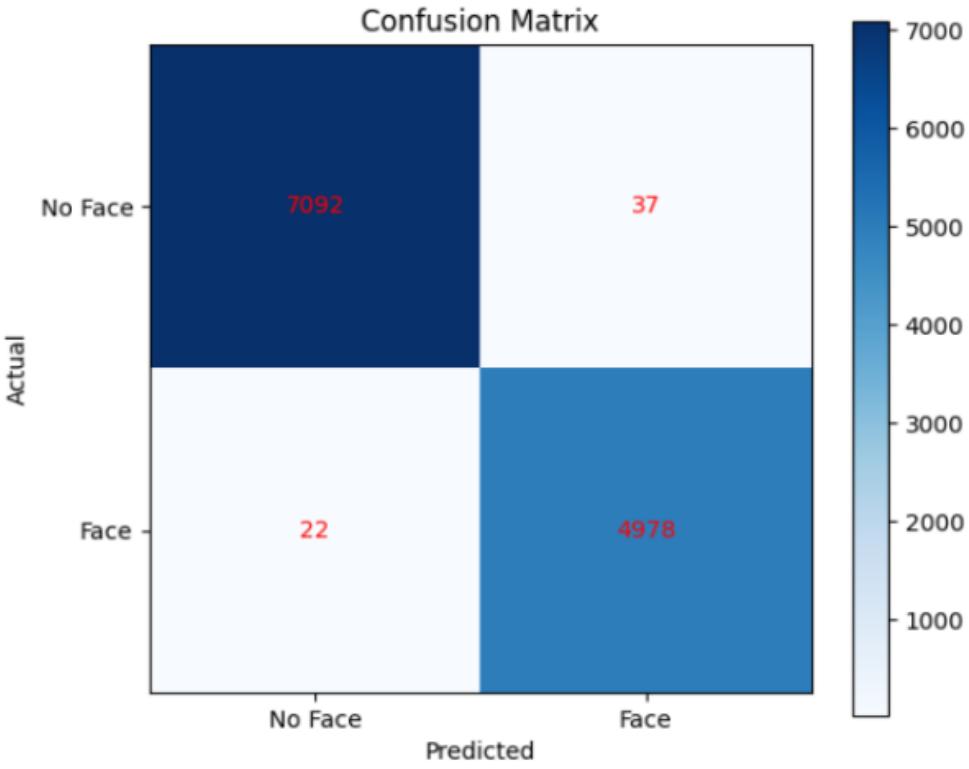

Figure 5.2: confusion matrix of Testing Face Detection System

From these values, the following metrics were calculated

- **Accuracy** measures proportion of correctly classified instances among all samples:

$$0.9951 \approx \frac{12070}{12129} = \frac{4978 + 7092}{4978 + 7092 + 37 + 22} = \frac{TP + TN}{TP + TN + FP + FN} = Accuracy$$

- **Precision** indicates the proportion of true positives among all predicted positives:

$$0.9926 \approx \frac{4978}{5015} = \frac{4978}{4978 + 37} = \frac{TP}{TP + FP} = Precision$$

- **Recall** measures the proportion of true positives detected among all actual positives

$$0.9956 \approx \frac{4978}{5000} = \frac{4978}{4978 + 22} = \frac{TP}{TP + FN} = Recall$$

- **F1-Score** is the harmonic mean of precision and recall:

$$0.9941 \approx \frac{0.9926 \times 0.9956}{0.9926 + 0.9956} \times 2 = \frac{Precision \times Recall}{Precision + Recall} \times 2 = F1 - Score$$

These values demonstrate that the MTCNN model performed with high precision and recall on our diverse test dataset, accurately identifying faces in nearly all images.

5.2.2.4 Analyzing Results

The analysis of the results obtained from the MTCNN-based face detection system highlights its reliability and robustness in detecting human faces under varied conditions. With an **accuracy of approximately 99.5%**, the model successfully processed the vast majority of the test images, producing minimal false classifications.

The high precision (99.26%) indicates that the system rarely misclassifies non-face images as containing faces, which is crucial in access control applications to avoid granting unnecessary access or initiating recognition on irrelevant input.

Likewise, **the recall (99.56%)** reflects the model's strong capability to detect nearly all actual faces in the dataset, minimizing the risk of missed detections.

The F1-score of 99.41% confirms a strong balance between precision and recall, reinforcing the model's suitability for real-time deployment. Despite the excellent performance, a small number of false positives (37) and false negatives (22) were recorded. These could be attributed to factors such as image quality, occlusions, or edge cases involving partial faces or ambiguous objects resembling facial features.

Overall, these findings support the integration of MTCNN as the face detection backbone in our system and validate its effectiveness across various image scenarios.

5.2.3 Face Recognition System Testing

This section presents the evaluation of the Face Recognition System, which is a core component of our access control architecture. The goal of this experiment is to assess the models ability to correctly identify individuals based on their facial embeddings and make accurate decisions regarding access authorization. The system was tested using a dataset of known and unknown faces under various conditions to verify its robustness and reliability.

5.2.3.1 Testing Method

To evaluate the Face Recognition System, we employed a two-stage approach consisting of face detection followed by face embedding and comparison, which this the method in our project. The first stage involved using a pre-trained MTCNN (Multi-task Cascaded Convolutional Networks) model to detect and crop faces from images.The second stage used the FaceNet model, based on the InceptionResNetV1 architecture and pre-trained on the VGGFace2 dataset, to extract feature embeddings from the detected faces.

Each detected face embedding was then compared against a database of known embeddings using Euclidean distance. A prediction was considered correct if the embedding of the detected face matched the correct identity from the database, verified through filename correspondence. This matching process simulates a real-world scenario where a captured face is checked against stored identities to determine recognition accuracy.

5.2.3.2 Data Preparation

The testing dataset consisted of 5,000 facial images obtained from the Kaggle platform. From this set, a random subset of 2,500 images was selected to form the face database, representing known identities with which comparisons were made. The remaining 5,000 images served as the query images, simulating live captures to be recognized.

For each query image, the system attempted to detect the face, extract its embedding, and search for a matching identity in the database. A successful recognition was determined by comparing the query images filename with that of the closest match found in the database. If both filenames matched, the prediction was labeled as correct (True Positive); otherwise, it was considered incorrect (False Positive or False Negative, depending on context).

5.2.3.3 Calculating Results

To assess the performance of the Face Recognition System, standard classification metrics were computed based on the confusion matrix results:
True Positives (TP): 2,496
True Negatives (TN): 12,456,282
False Positives (FP): 14
False Negatives (FN): 0

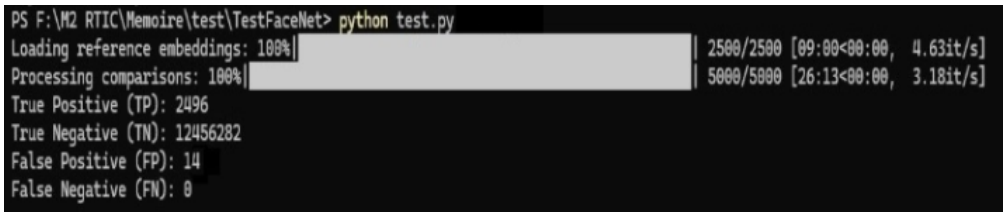

Figure 5.3: confusion matrix of Testing Mobile Screen Detection System2

Using these values, the following metrics were calculated:

- **Accuracy** measures proportion of correctly classified instances among all samples:

$$0.999998 \approx \frac{123456282 + 2496}{0 + 14 + 123456282 + 2496} = \frac{TP + TN}{TP + TN + FP + FN} = Accuracy$$

- **Precision** indicates the proportion of true positives among all predicted positives:

$$0.9944 \approx \frac{2496}{14 + 2496} = \frac{TP}{TP + FP} = Precision$$

- **Recall** measures the proportion of true positives detected among all actual positives

$$1.000000 \approx \frac{2496}{0 + 2496} = \frac{TP}{TP + FN} = Recall$$

- **F1-Score** is the harmonic mean of precision and recall:

$$0.9972 \approx \frac{1.0000 \times 0.9944}{1.0000 + 0.9944} \times 2 = \frac{Precision \times Recall}{Precision + Recall} \times 2 = F1 - Score$$

5.2.3.4 Analyzing Results

The performance metrics achieved by the face recognition system are a clear testament to the exceptional robustness and precision of the integrated model based on MTCNN for face detection and FaceNet for face recognition, leveraging the powerful InceptionResNetV1 architecture pretrained on the VGGFace2 dataset.

With an **accuracy of 99.9998%**, the system demonstrates an extraordinary ability to correctly classify both matching and non-matching facial identities across over 12 million comparisons. This metric alone positions the model among the most reliable and scalable face recognition systems currently available in the field of biometric authentication.

Moreover, **the precision of 99.44%**underscores the systems remarkable capability to avoid false positives, ensuring that identities are not mistakenly accepteda crucial aspect in high-security environments. This level of precision reflects a system that not only performs well statistically, but also upholds the integrity of real-world access control mechanisms.

The perfect **recall score of 100%** is particularly impressive, as it indicates that the model did not miss a single true identity present in the database. This means that every legitimate individual was successfully recognized, demonstrating the model's excellence in feature extraction and comparison under real-world constraints.

Finally, **the F1-score of 99.72%** encapsulates the model's balanced excellence in both sensitivity and specificity. It reflects a solution that does not trade off one metric for another, but instead achieves harmony across all fronts.

In summary, the **MTCNNFaceNet** pipeline can only be described as a formidable giant in the realm of facial recognition. Its performance in this study confirms not only the soundness of its architectural design, but also its practical readiness for deployment in mission-critical applications such as smart access control, surveillance, and high-security verification systems.

This model is not just an algorithmit is a **masterfully engineered system**, capable of real-time identification with surgical precision. Its performance here elevates it to the status of a cornerstone technology in intelligent security systems.

5.3 Conclusion

The results presented in this chapter stand as undeniable proof of the exceptional power, precision, and intelligence embedded within the proposed access control system. Each component, from the spoofing prevention module to the face recognition engine, has not only met expectations but vastly surpassed them.

The mobile screen detection system, based on the YOLOv8s architecture, demonstrated lightning-fast inference and incredible classification accuracy, forming an impenetrable front line against deception attempts using phones or displays. Its performance metrics were not just highthey were exceptional, reflecting a level of reliability that is rarely seen in real-time detection systems.

On the other hand, the face recognition module, powered by MTCNN and FaceNets InceptionResNetV1, emerged as a truly elite biometric solution. Its ability to perform over 12 million comparisons with zero false negatives and near-zero false positives is not just impressiveit is a monumental technological achievement. This system doesn't guess it recognizes with surgical precision.

Together, these AI-powered modules form a cohesive and intelligent gatekeeping system that delivers on all fronts: security, speed, scalability, and stability. The results obtained are not merely good they are extraordinary, highlighting the system's potential to reshape the future of access control technologies.

This chapter proves, without any doubt, that the proposed system is not a prototype it is a powerful, production-ready solution, capable of securing high-sensitivity environments with unmatched efficiency and scientific brilliance.

Chapter 6

General Conclusion

In this thesis, we explored the design, development, and deployment of an intelligent door access system based on facial recognition, with the motivation to enhance security through modern artificial intelligence techniques and embedded systems. Beginning with a comprehensive contextual and theoretical background, we discussed the concepts of facial recognition technologies, their evolution, and incorporation into various security systems. Current system analysis showed the strengths as well as the shortcomings of traditional and biometric-based systems, revealing the growing need for more secure, smart, and convenient access control systems.

The implementation phase of our project involved the creation of a sound architecture incorporating computer vision, deep learning algorithms, and IoT elements through the use of Raspberry Pi. We used a multi-step process involving face detection via MTCNN, feature extraction and recognition via FaceNet, and liveness detection via eye blinking (EAR) to avoid spoofing. Not only was the prototype developed working, but it was also efficient for real-time applications following extensive testing and analysis.

With the experimental results, we verified and validated the efficiency and reliability of our system under varying conditions, demonstrating the viability of our solution. Despite some limitations with respect to light conditions, user positioning, or hardware constraints, the system overall demonstrates a solid alternative to conventional access control techniques.

In conclusion, this project illustrates the viability of combining AI and embedded systems in tackling real-world security problems. Future projects can attempt to improve the recognition under different conditions, enhance user privacy, and augment the system with additional sensors, whether they are biometric or environmental, for even more robust performance.

Bibliography

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2011). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[2] P. Timse et al.Face recognition based door lock system using opencv and C# with remote access and security features Int. J. Eng. Res. Appl.(2014)

[3] L. Zhang An improved approach to security and privacy of RFID application system

[4] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM Computing Surveys (CSUR), 35(4), 399-458.

[5] S. Pawar et al. Smart home security using IoT and face recognition

[6] Li, S. Z., & Jain, A. K. (2011). Handbook of face recognition. Springer.

[7] A. Nag et al. IOT based door access control using face recognition

[8] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. British Machine Vision Conference.

[9] J. Copeland, Artificial Intelligence: A Philosophical Introduction, 1st ed. Massachusetts: Blackwell Publishers, 1993.

[10] E.Lance and E.Michael, Autonomous Vehicle Driverless Self-Driving Cars and Artificial Intelligence: Practical Advances in AI and Machine Learning, 1st ed. LBE Press Publishing, 2014.

[11] S.Milan, H.Vaclav, and B.Roger, Image Processing, Analysis, and Machine Vision, 4th ed. Cengage Learning, 2014.

[12] Thorat SB, Head SKN, Jyoti M, et al. Facial recognition technology: an analysis with scope in India. Int J Comput Sci Inf Secur 2010; 8: 325330.

[13] Goldstein BAJ, Harmon LD and Lesk AB. Man machine interaction in human-face identification. Bell Syst Tech J 1972; 51: 399427.

[14] Sirovich L and Kirby M. Low-dimensional procedure for the characterization of human faces. J Opt Soc Am A 1987; 4: 519.

[15] Matthew T and Pentland A. Eigenfaces for recognition. J Cogn Neurosci 1991; 3: 7189.

[16] Fontaine X, Achanta R and Susstrunk S. Face recogni tion in real-world images. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, 59 March 2017, pp.14821486. Piscataway, NJ: IEEE.

[17] Shukla S and Dave S. Comparison of face recognition algorithms and its subsequent impact on side face. In: International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 1819 November 2016, pp.18. Piscataway: IEEE.

[18] Kaur P, Krishan K, Sharma SK, et al. Integrating a pro f ile of frontal face with its mirror image for facial recon struction. J Craniofac Surg 2018; 29: 10261030.

[19] G. Thomson, Facial Recognition, Encyclopedia, 2005. [Online]. Available: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/facialrecognition. [Accessed: 11-Oct-2018].

[20] M. Kafai, L. An, and B. Bhanu, Reference face graph for face recognition, IEEE Trans. Inf. Forensics Secur., vol. 9, no. 12, pp. 21322143, 2014.

[21] S. Zhaoqing, Z. Su, and L. I. Zhicheng, Face Images Recognition Research Based on Smooth Filter and Support Vector Machine *, pp. 27602764, 2010.

[22] M. Arsenovic, S. Sladojevic, A. Anderla, and D. Stefanovic, FaceTime - Deep learning based face recognition attendance system, SISY 2017 - IEEE 15th Int. Symp. Intell. Syst. Informatics, Proc., pp. 5357, 2017

[23] Facial Recognition Technology: A Comprehensive Overview (Li Qinjun*, Cui Tianwei, Zhao Yan, Wu Yuying)

[24] Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics, 9(8), 1188.

[25] Sengupta, S., Chen, J. C., Castillo, C., Patel, V. M., & Jacobs, D. W.. (2016). Frontal to profile face verification in the wild. 2016 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE

[26] Zhou, S., Xiao, S. (2018). 3D face recognition: a survey. Hum. Cent. Comput. Inf. Sci. 8, 35.

[27] Luo, J., Hu, F., & Wang, R. (2019). 3D face recognition based on deep learning. In 2019 IEEE International Conference on Mechatronics and Automation (ICMA) (pp. 1576-1581). IEEE

[28] Rajpurkar, O. M., Kamble, S. S., Nandagiri, J. P., & Bide, P. J. (2020). A Survey on Engagement and Emotion Analysis in Theatre using Thermal Imaging. 2020 4th International Conference on Published by Francis Academic Press, UK -24- Academic

Journal of Computing & Information Science ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703 Electronics, Communication and Aerospace Technology (ICECA).

[29] Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., ... & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. Journal of Law and the Biosciences, 7(1), lsaa038.

[30] FACIAL FEATURE EXTRACTION TECHNIQUES FOR FACE RECOGNITION (Rahib H. Abiyev)

[31] Face Image Feature Extraction based on Deep Learning Algorithm (Qing Kuang)

[32] . Zhao W, Chellappa R, Phillips PJ, Rosenfeld A (2003) Face recognition: a literature survey. ACM Comput Surv (CSUR) 35(4):399458

[33] . Roberts LG (1963) Machine perception of three-dimensional solids. Ph.D. thesis Massachusetts Institute of Technology

[34] . Kanade T (1973) Picture processing system by computer complex and recognition of human faces. Ph.D. thesis, Kyoto University, Japan

[35] . Arashloo SR (2016) A comparison of deep multilayer networks and markov random field matching models for face recognition in the wild. IET Comput Vis 10(6):466474

[36] . Sun Y, Wang X, Tang X (2013) Hybrid deep learning for face verification. In: IEEE International conference on computer vision, ICCV, Sydney, pp 14891496

[37] . Plenge E, Klein SS, Niessen WJ, Meijering E (2015) Multiple sparse representations classification. PLOS ONE10(7):123

[38] . Zadeh LA (1965) Fuzzy sets. Inf Control 8(3):338353

[39] . Singh M and Arora AS. Varying illumination and pose conditions in face recognition. Procedia Comput Sci 2016; 85: 691695.

[40] . Zhang X and Gao Y. Face recognition across pose: a review. Pattern Recognit 2009; 42: 28762896.

[41] . Sharma M, Prakash S and Gupta P. An efficient partial occluded face recognition system. Neurocomputing 2013; 116: 231241.

[42] . Samadiani N, Huang G, Cai B, et al. A review on auto matic facial expression recognition systems assisted by multimodal sensor data. Sensors 2019; 19: 1863.

[43] . Li X and Da F. Efficient 3D face recognition handling facial expression and hair occlusion. Image Vis Comput 2012; 30: 668679. 25. Marques I. Face recognition algorithms. Masters Thesis. Universidad Euskal Herriko, Spain, 2010.

[44] . Abate AF, Nappi M, Riccio D, et al. 2D and 3D face recognition: a survey. Pattern Recognit Lett 2007; 28: 18851906.

[45] Lu, C. , & Tang, X. . (2014). Surpassing human-level face verification performance on lfw with gaussianface. Computer Science.

[46] Bashbaghi, S. , Granger, E. , Sabourin, R. , & Parchami, M. (2018). Deep Learning Architectures for Face Recognition in Video Surveillance. 10.48550/arXiv.1802.09990.

[47] Hebbale, S. G. , Mukherjee, A. , & Seal, A. . (2019). People Search on Social Media Platform Using Face Recognition. SoutheastCon 2019.

[48] Herlitz, A., & Lovén, J. (2013). Sex differences and the own-gender bias in face recognition: A meta-analytic review. Visual Cognition, 21(9-10), 1306-1336.

[49] Bowyer, K. W. (2004). Face recognition technology: security versus privacy. IEEE Technology and society magazine, 23(1), 9-19.

[50] Senior, A. W., & Pankanti, S. (2011). Privacy protection and face recognition. Handbook of face recognition, 671-691.

[51] Pragya Gupta, A. M. Gopi, and Harleen Kaur, "Recent Trends in Deep Learning Based Face Recognition," in *Advances in Data Computing, Communication and Security*, Springer, Singapore, 2024, pp. 2333. Available: link

[52] Recent Advances in Deep Learning Techniques for Face Recognition By: MD. TAHMID HASAN FUAD 1,AWALAHMEDFIME1, DELOWAR SIKDER1, MD. AKIL RAIHAN IFTEE1, JAKARIA RABBI 1,MABROOK S. AL-RAKHAMI OVISHAKE SEN 2,(Senior Member, IEEE), ABDU GUMAEI 1,MOHTASIM FUAD1, AND MD. NAZRUL ISLAM1

[53] Wang, M., Luo, H., & Cheng, J. C. (2021). Towards an automated condition assessment framework of underground sewer pipes based on closed-circuit television (CCTV) images. Tunnelling and Underground Space Technology, 110, 103840.

[54] Ullah, Z., Al-Turjman, F., Mostarda, L., &Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. Computer Communications, 154, 313-323.

[55] Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, 113114.

[56] Alsadie, D. (2024). Artificial intelligence techniques for securing fog computing environments: trends,challenges, and future directions. IEEE Access.

[57] Towne, S. C. H. U. Y. L. E. R. (2018). Rethinking the Origins of the Lock.

[58] Deibert, R., Palfrey, J., Rohozinski, R., &Zittrain, J. (2010). Access controlled: The shaping of power, rights, and rule in cyberspace (p. 634). the MIT Press.

[59] Pace, T. D. (2014). A typology of Roman locks and keys (Doctoral dissertation, Southwestern Baptist Theological Seminary).

[60] Pulford, G. (2007). High-security mechanical locks: an encyclopedic reference. Butterworth-Heinemann.

[61] Farrell, G., & Tilley, N. (2022). Elegant security: Concept, evidence and implications. European Journal of Criminology, 19(5), 932-953.

[62] Fadlianda, D., &Fikry, M. (2024, December). Innovative IoT-Based Automatic Gate System with RFID and Electro-Magnetic Lock for Secure Access. In Proceedings of Malikussaleh International Conference on Multidisciplinary Studies (MICoMS) (Vol. 4, pp. 00005-00005).

[63] Goffer, M. A., Hasan, S. N., Das, N., Kaur, J., Hassan, J., Barikdar, C. R., & Das, S. (2025). Cybersecurity and Supply Chain Integrity: Evaluating the Economic Consequences of Vulnerabilities in US Infrastructure. Journal of Management World, 2, 233-243.

[64] Sehgal, N. K., Saxena, M., & Shah, D. N. (2024). AI on the Edge with Security. Springer Nature.

[65] Konheim, A. G. (2016). Automated teller machines: their history and authentication protocols. Journal of Cryptographic Engineering, 6(1), 1-29.

[66] Adebimpe, L. A., Ng, I. O., Idris, M. Y. I., Okmi, M., Ku, C. S., Ang, T. F., &Por, L. Y. (2023). Systemic literature review of recognition-based authentication method resistivity to shoulder-surfing attacks. Applied Sciences, 13(18), 10040.

[67] Kumar, A., Yadav, B., Jopre, A., &Deshmukh, M. (2025). Multi-Protocol Communication and Security System Using ESP8266/32. International Journal of Innovative Science and Research Technology, 10(3), 471-480.

[68] Anusha, R., Shankari, N., Surabhi, S. S., Srijan, S. U., &Yashwin, K. S. (2025, March). An IoT Based Access Control System Using R307 Optical Biometric Sensor. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1759-1764). IEEE.

[69] Prakasha, K. K., &Sumalatha, U. (2025). Privacy-Preserving Techniques in Biometric Systems: Approaches and Challenges. IEEE Access.

[70] Maheswaran, S., Gomathi, R. D., Rithikhaa, D., Praveen, B., Prathiksha, T., Murugesan, G., &Nandita, S. (2023, July). A Perspective way of designing Intelligent systems with Face Detection and Recognition using Artificial Intelligence for Authentication.

In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[71] Lakshumiah, A., Malaiarasan, A., Packianathan, R., Natarajan, S. K., &Arumugam, G. (2025). Application of Artificial Intelligence (AI) Techniques for Green Transportation in Smart City. In Driving Green Transportation System Through Artificial Intelligence and Automation: Approaches, Technologies and Applications (pp. 335-358). Cham: Springer Nature Switzerland.

[72] Azad, M. M., Kim, S., Cheon, Y. B., & Kim, H. S. (2024). Intelligent structural health monitoring of composite structures using machine learning, deep learning, and transfer learning: a review. Advanced Composite Materials, 33(2), 162-188.

[73] Asaithambi, S. P. R., Venkatraman, S., &Venkatraman, R. (2021). Proposed big data architecture for facial recognition using machine learning. AIMS Electronics and Electrical Engineering, 5(1), 68-92.

[74] Alanno, A. A. A. (2020). Machine learning implementation in face recognition and identification.

[75] Gibert, D., Planes, J., Mateu, C., & Le, Q. (2022). Fusing feature engineering and deep learning: A case study for malware classification. Expert Systems with Applications, 207, 117957.

[76] Nahavandi, S., Alizadehsani, R., Nahavandi, D., Mohamed, S., Mohajer, N., Rokonuzzaman, M., & Hossain, I. (2022). A comprehensive review on autonomous navigation. ACM Computing Surveys.

[77] Paul, A. K. (2024). FaceLite: A Real-Time Light-Weight Facemask Detection Using Deep Learning: A Comprehensive Analysis, Opportunities, and Challenges for Edge Computing. Computer Networks and Communications, 83-111.

[78] Lee, J. H., Yu, H. J., Kim, M. J., Kim, J. W., & Choi, J. (2020). Automated cephalometric landmark detection with confidence regions using Bayesian convolutional neural networks. BMC oral health, 20, 1-10.

[79] [29]Elharrouss, O., Almaadeed, N., Al-Maadeed, S.,&Khelifi, F. (2022). Pose-invariant face recognition with multitask cascade networks. Neural Computing and Applications, 1-14.

[80] Harrabi, R., CHAABANE, S. A. E. B., &Seddik, H. S. (2025). Hybrid Approach for Face Recognition Using Convolutional Neural Networks, Fuzzy Logic, and SVM Classifier.

[81] Li, Z., Zhang, H., Wang, J., Chen, M., Hu, H., Yi, W., ...& Ma, C. (2025). From Head to Tail: Efficient Black-box Model Inversion Attack via Long-tailed Learning. arXiv preprint arXiv:2503.16266.

[82] Gholizade, M., Soltanizadeh, H., Rahmanimanesh, M., & Sana, S. S. (2025). A review of recent advances and strategies in transfer learning. International Journal of System Assurance Engineering and Management, 1-40.

[83] Gholizade, M., Soltanizadeh, H., Rahmanimanesh, M., & Sana, S. S. (2025). A review of recent advances and strategies in transfer learning. International Journal of System Assurance Engineering and Management, 1-40.

[84] Gholizade, M., Soltanizadeh, H., Rahmanimanesh, M., & Sana, S. S. (2025). A review of recent advances and strategies in transfer learning. International Journal of System Assurance Engineering and Management, 1-40.

[85] Gholizade, M., Soltanizadeh, H., Rahmanimanesh, M., & Sana, S. S. (2025). A review of recent advances and strategies in transfer learning. International Journal of System Assurance Engineering and Management, 1-40.

[86] Chaganti, K. C. (2025). A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches. IEEE Access.

[87] Harkai, A., &Ciurea, C. E. (2024). Economic impact of IOT and conventional data breaches: cost analysis and statistical trends. Control & Cybernetics, 53(2).

[88] Yen, M. H., Mishra, N., Luo, W. J., & Lin, C. E. (2025). A Novel Proactive AI-Based Agents Framework for an IoE-Based Smart Things Monitoring System with Applications for Smart Vehicles. Computers, Materials & Continua, 82(2).

[89] Penica, M., Bhattacharya, M., OBrien, W., McGrath, S., Hayes, M., & OConnell, E. (2025). Advancing Interoperable IoT-Based Access Control Systems: A Unified Security Approach in Diverse Environments. IEEE Access.

[90] Kassim, M. S. M., bin Rozman, M. H., &Yahya, F. (2025, January). Frozen Food Supply Chain Monitoring with IoT. In 2025 19th International Conference on Ubiquitous Information Management and Communication (IMCOM) (pp. 1-6). IEEE.

[91] Kaspersky. What is facial recognition? Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition [Accessed: 21-May-2025].

[92] Different Types of Door Access Control Systems [Accessed: 2025].

[93] Guide to Key Card Entry Systems [Accessed: 2025].

[94] deep-learning.html [Accessed: 2025].

[95] what-is-transfer-learning [Accessed: 2025].

[96] transfer-learning-in-deep-learning-leveraging-pre-trained-models-for-faster-and-better-training [Accessed: 2025].

[97] introduction-to-transfer-learning [Accessed: 2025].

[98] transfer-learning [Accessed: 2025].

[99] solenoid-electromagnetic-lock . [Accessed: 2025].

[100] Electronics-White-Breadboard [Accessed: 2025].

[101] LCD16X2 [Accessed: 2025].

[102] Ultrasonic Sensor [Accessed: 2025].

[103] LEDs [Accessed: 2025].

[104] Buzzer [Accessed: 2025].

[105] 5v-1-channel-relay-module [Accessed: 2025].

[106] visual Studio [Accessed: 2025].

[107] Python. [Accessed: 2025].

[108] Flask icon [Accessed: 2025].

[109] tinkercad. [Accessed: 2025].

[110] HTML [Accessed: 2025].

[111] CSS [Accessed: 2025].

[112] javascript-logo-png [Accessed: 2025].

[113] Raspberrypi [Accessed: 2025].

[114] Building Real-Time Face Recognition with Python | by Suditi Gupta | Medium [Accessed: 2025].

[115] how-to-use-facial-recognition [Accessed:].

[116] Eye blinking detection with Python and OpenCV Pysource (2019) [Accessed: 2025].

[117] Eye blink detection with OpenCV and dlib PyImageSearch (2017) [Accessed: 2025].

[118] Eye blinking detection in videos with dlib & OpenCV DataHacker (2020) [Accessed: 2025].

[119] The Anycubic i3 Mega 3D printer. . [Accessed: 2025].

[120] fritzing. [Accessed: 2025].

[121] TigerVNC Viewer[Accessed: 2025]

[122] Xampp [Accessed: 2025]