Secure Cloud Based Biometric Authentication

A major project report submitted in partial fulfillment of the requirement for the award of degree of

Bachelor of Technology

in

Computer Science & Engineering / Information Technology

Submitted by

Shrutika (201223)

Devansh Barki(201242)

Under the guidance & supervision of

Dr. Pradeep Kumar

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology, Waknaghat, Solan - 173234 (India)

Certificate

This is to certify that the work which is being presented in the project report titled “Secure Cloud Based Biometeric Authentication” in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of work carried out by “ Shrutika , 201223 ” “Devansh Barki , 201242” during the period from January 2024 to May 2024 under the supervision of Dr. Pardeep Kumar , Department of Computer Science and Engineering, Jaypee University of Information Technology,Waknaghat.

Shrutika (201223)

Devansh Barki (201242)

The above statement made is correct to the best of my knowledge.

Dr. Pardeep Kumar
Associate Professor
Computer Science &Engineering and Information Technology
Jaypee University of Information Technology, Waknaghat,

Candidate’s Declaration

We hereby declare that the work presented in this report entitled **‘Secure Cloud Based Biometric Authentication’** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science & Engineering / Information Technology** submitted in the Department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology, Waknaghat is an authentic record of our own work carried out over a period from January 2024 to May 2024 under the supervision of **Dr. Pardeep Kumar** (Associate Professor, Department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Shrutika(201223)
Devansh Barki(201242)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

Dr. Pradeep Kumar
Associate Professor
Computer Science And Engineering
Dated :

ACKNOWLEDGEMENT

We would like to express my deepest appreciation to Dr. Pardeep Kumar for helping us throughout the project and without whom this project would have been a very difficult task. We are highly indebted to ma’am for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in doing the project. He consistently motivated and guided us towards the completion of the project. We would like to express our gratitude towards my parents & members of JUIT for their kind cooperation and encouragement which helped us in doing this project. Our thanks and appreciations also go to our colleagues who have helped us out with their abilities in developing the project.

Devansh Barki
(201242)

Shrutika
(201223)

Table of Content

List of Tables

List of Figures

List of Abbreviations, Symbols or Nomenclature

3DES : Triple Data Encryption Algorithms

MD5 : Message Digest Algorithm

MM: Minute Map Algorithm

DWT : discrete wavelet transform

CPIO : continuous pigeon inspired optimizer

AWS :Amazon Web Services

IBDO :Identity-based data outsourcing

Abstract

Robust and secure authentication techniques are becoming increasingly important as the digital landscape changes. The primary objective of this project is to design and build a safe cloud-based biometric authentication system in order to enhance identity verification processes. Biometric authentication presents a viable way to address the problems associated with traditional authentication by utilizing each person's distinct physiological and behavioral traits.

The suggested system makes use of cloud infrastructure to handle and store biometric data, offering an expandable and easily accessible platform for authentication needs. Biometric data, like voice patterns, fingerprints, or facial features, is recorded and encrypted before being sent to the cloud in order to safeguard sensitive information's integrity and privacy. To protect the data during transmission and storage, sophisticated encryption protocols and secure communication channels are used.

The major objectives of the project are to create a user-friendly interface for biometric data collection, integrate it with the existing cloud services, and increase security by incorporating multi-factor authentication.The system incorporates machine learning algorithms to enhance and modify its accuracy in recognising and verifying biometric characteristics on a continuous basis.

Chapter 1: Introduction

1.1 Introduction

Biometric authorization is an alternative, transformative method that differs significantly from traditional authorization means such as passwords and personal identification numbers (PINs). It relies on body or behavioral features, which uniquely characterize an individual. They include but are not limited to fingerprints,

The latest example comes in the form of integrating biometric authentication with cloud-hosted platforms. Unlike on-premises hardware solutions, cloud-based biometric authentication enhances scalability and accessibility by reducing the reliance on local infrastructure. Users can seamlessly authenticate their identity from various internet-connected devices, underscoring the system's convenience without compromising security.

Central to the success of cloud-based biometric authentication is its commitment to robust security measures. Modern encryption methods are essential for protecting private biometric data kept on cloud servers.. The conversion of biometric information into a digital format ensures secure storage, with access restricted to authorized entities. This emphasis on privacy is fundamental for building user trust and fostering wider acceptance of biometric authentication systems.

The cloud-based architecture enhances security by enabling real-time updates and maintenance, a dynamic feature that allows the system to adapt swiftly to emerging security threats. Cloud-based solutions, in contrast to static, on-premises systems, can easily apply security patches and updates, guaranteeing that the authentication procedure stays reliable and current.

The convenience and accessibility of cloud-based biometric authentication are evident in its ability to operate across diverse devices. In addition to conventional desktop computers, users can authenticate their identity using smartphones, tablets, and other linked devices. This multidevice capability enhances user flexibility, catering to the varied ways individuals engage with digital services in our interconnected world.

In conclusion, cloud-based biometric authentication represents a secure and convenient response to identity verification challenges in our connected society. The amalgamation of cutting-edge encryption, cloud infrastructure, and real-time adaptability positions this innovative approach at the forefront of creating a more convenient and secure digital future. As the digital landscape continues to evolve, cloud-based biometric authentication serves as a testament to ongoing efforts to prioritize both security and user experience in identity verification systems. The integration of these technologies marks a significant stride toward establishing a robust, reliable, and user-friendly approach to identity verification in our interconnected and digitized world.

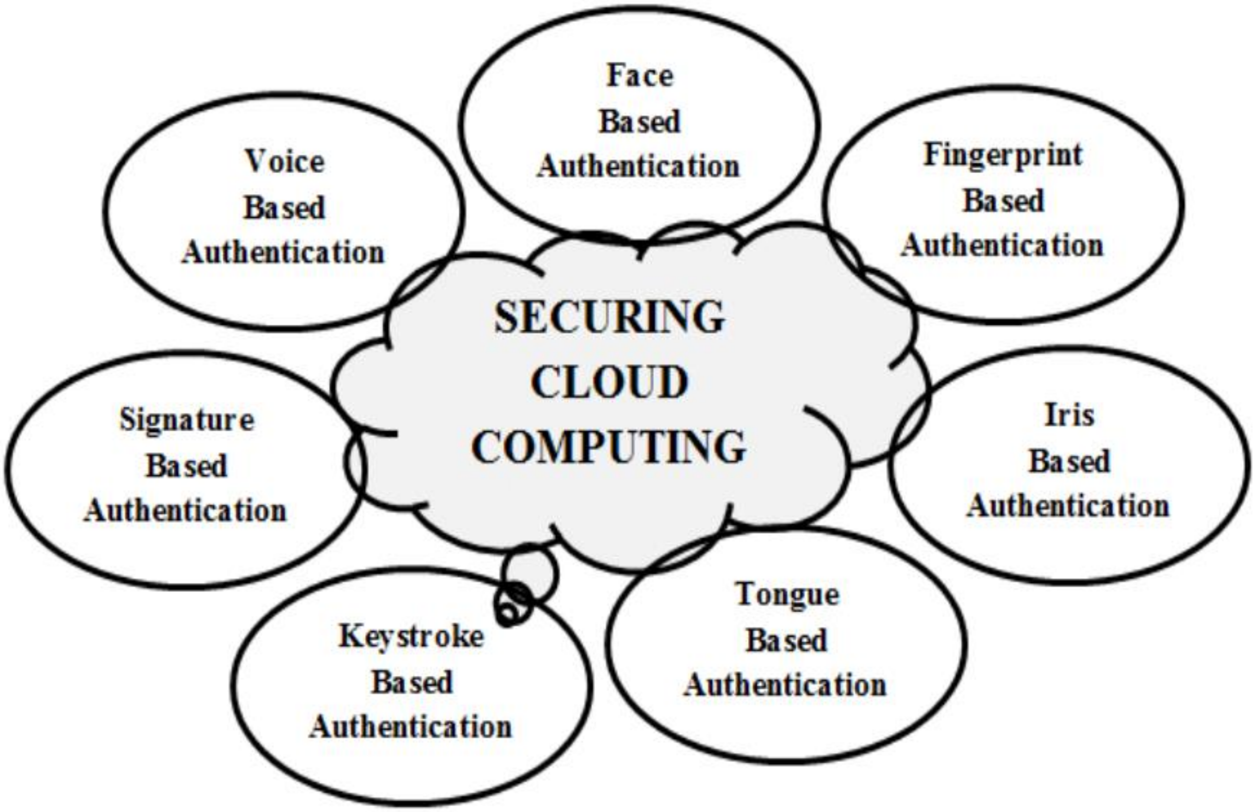

Face Based Authentication
Voice Based Authentication
Fingerprint Based Authentication
SECURING CLOUD COMPUTING
Signature Based Authentication
Iris Based Authentication
Keystroke Based Authentication
Tongue Based Authentication

Figure 1.1: Types of Biometric Authentication [15]

1.2 Problem Statement

The main difficulty we have with cloud-based biometric authentication is striking the correct balance between security and ease of use. Although it would be very simple to access your accounts using just your face or fingerprints, we must ensure that sensitive data, such as fingerprints, is secure when transferred online.. Consider it akin to a sophisticated secret code that deters hackers. Thus, ensuring that robust security protocols are in place to safeguard this unique data both during storage and transmission across the internet presents a significant challenge.

Getting people to feel at ease utilizing this new identity-proving method is another challenging aspect. Since we've been using passwords for a while, trying anything new can be a little scary. We must thus educate people about how incredibly safe and user-friendly this technology is. We want them to feel secure knowing that their personal information is secure. Lastly, we want to ensure that this system runs perfectly on a variety of devices, such as phones and PCs. To do that, we must establish uniform guidelines and standards that guarantee a dependable and safe experience regardless of the device being used. Solving these challenges is essential to making cloud-based biometric authentication widely accepted and secure, creating a future where proving your identity is both easy and safe.

1.3 Objectives

- To design a platform which is able to strengthen cloud service security by implementing biometric authentication.
- To Build a system that provides accurate biometric recognition algorithms for user identification.
- To develop strong encryption mechanisms and secure storage protocols to safeguard biometric data from unauthorized access or tampering.
- To design a seamless and user-friendly biometric authentication process.

- To provide a thorough education and awareness programme aimed at system operators, administrators, and end users with the goal of increasing responsible usage of the biometric authentication system and developing a thorough understanding of the security mechanisms in place.
- To combine biometrics with extra layers of verification in multi-factor authentication techniques, thereby strengthening the cloud-based platform's overall security posture.
- To create transparent and unambiguous privacy policies that tell users about the uses, storage, and protection of their biometric data in order to build user trust and encourage adherence to data protection laws.

1.4 Significance and Motivation of the Project Work

Because secure cloud-based biometric authentication has such a profound effect on digital security and user experience, its importance is multifaceted and crosses multiple domains.

- By adding an additional layer of security, biometric authentication makes sure that only people with permission can access sensitive data kept in the cloud.
- **Convenience and Ease of Use:** Users can authenticate themselves through their biometric traits, eliminating the need to remember complex passwords or carry physical tokens.
- **Cost-Effectiveness:** Cloud-based authentication reduces infrastructure costs, as organizations can leverage third-party services and pay for the resources they actually use.
- **Scalability and Flexibility:** Cloud-based solutions can easily scale to accommodate growing user demands, offering the flexibility to adapt to changing security requirements.
- **Global Accessibility:** Cloud-based solutions encourage global accessibility and lessen geographic limitations by allowing users to access their accounts or resources from almost anywhere with an internet connection.

- **Enhanced Fraud Detection:**An additional line of protection against fraudulent attempts to access sensitive data is provided by the system's ability to identify anomalies or inconsistencies through the ongoing monitoring of biometric traits.

The following important factors underpin the project's motivation for secure cloud-based biometric authentication and highlight its importance and necessity:

- **Cyber Security Concerns:** Biometric characteristics, as opposed to static passwords, allow for continuous user identity assurance throughout a session. Security is further strengthened by this dynamic authentication.
- **User-Friendly Authentication:** The probability of common password-related problems like shared passwords, forgotten passwords, and password-based attacks like phishing is decreased by biometric authentication.
- **Global Accessibility:** Fulfilling the demand for globally accessible authentication systems that represent the interconnectedness of digital services.
- **Technological Advancements:** Utilizing hardware capabilities and biometric recognition algorithm advancements to increase accuracy and dependability.
- **Mitigating Password-Related Risks:** Lowering the dangers connected to common password-related weaknesses like stolen credentials and weak passwords.
- **User Empowerment and Trust:** Empowering users by establishing trust in the protection of biometric data and the security and integrity of the authentication system.

1.5 Organization of Project Report

1. Chapter 01: Introduction The first chapter describes the essence of the project, defining aims and methodologies. It serves as the project's narrative, introducing the fundamental topic with brevity and depth. It thoughtfully outlines the project's concept, welcoming readers into an exciting world of AI-driven healthcare.

2. Chapter 02: Literature Review The second chapter does a literature study, evaluating academic works on "Secure Cloud Based Biometeric Authentication " in order to measure and compare our project outcomes to previous research. This thorough analysis expands our understanding of the subject issue, offering useful background and insights for our project.

3. Chapter 03 : System Development The project's system development takes center stage in this, with code samples, algorithms, and evaluation. It gives readers a thorough knowledge of the project's technological basis by providing a complete overview of system capabilities.

4. Chapter 04 : Testing provides light on the stringent evaluation techniques used, providing a clear insight into how the project's functioning gets evaluated.

5. Chapter 05 : Result and Evaluation This chapter evaluates if our project has reached its objectives and confirms that everything functions as it should. It's like a report card for our project, letting us know what worked and what didn't, as well as the overall success of our efforts.

6. Chapter 06 : Conclusion and Future Scope In this we discuss what went well and what we learned. Looking ahead, we talk about innovative ways to improve the project in the future.

Chapter 2: Literature Survey

2.1 Overview of Relevant Literature

2.1.1 “A Proposed BiometricAuthentication Model to Improve Cloud Systems Security”[1]

The article addresses the drawbacks of conventional username and password authentication methods and suggests a cloud-based biometric authentication model (CBioAM) to improve cloud system security. The suggested model, known as CBioAS, implements the authentication process without jeopardizing user data by storing biometric samples of users in database servers. The proposed model is implemented and evaluated using a novel algorithm called "Bio_Authen_as_a_Service," which is introduced in the paper. The experimental results show a 96.15% average accuracy, an 87.69% sensitivity, and a 97.99% specificity, indicating promising performance. By providing a biometric authentication process that is both secure and privacy-preserving for cloud services, the suggested model reduces the risks related to stolen or identified personal data.

2.1.2 “BAMCloud: a cloud based Mobile biometric authentication framework” [2]

The paper proposes BAMCloud, a high-performance cluster Cloud-based distributed mobile biometric system, to tackle the performance problems brought on by the growing number of biometric system registrants.BAMCloud uses data collected from handheld mobile devices for authentication and uses dynamic signatures. The system uses a distributed cloud-based approach to perform tasks including training, preprocessing, and data storage.BAMCloud is implemented using the Levenberg-Marquardt backpropagation neural network for training and MapReduce on the Hadoop platform for data processing.Competing with other methods in the latest research, the proposed framework achieves 96.23% performance and an 8.5x speedup.

2.1.3 ” Privacy preserving steganography based biometric authentication system for cloud computing environment” [3]

In this paper, a biometric authentication system (BAS) for cloud environments that preserves privacy through steganography is presented.Through encrypted transmission to the cloud, the PPS-BASE model seeks to blend the fingerprint image into the retinal image of the eye . Together with the continuous pigeon-inspired optimizer (CPIO) algorithm to identify the best pixel points in the cover image, the model uses the multilevel discrete wavelet transform (DWT) technique to split the cover image and identify the pixel location.

2.1.4 “Secure biometric authentication with deduplication on distributed cloud storage”[4]

The research study suggests a biometric authentication system that addresses data redundancy and grants users access permission in a cloud-distributed environment.Only authorized users can access the bio-key generated by the scheme using a cryptographic technique for authentication.The suggested technique generates the bio-key and stops data deduplication in the cloud by using a Gabor filter with distributed security and encryption using XOR operations, guaranteeing data redundancy avoidance and security.The study analyzes the deduplication performance of the suggested scheme by contrasting it with current algorithms and demonstrating that it requires less computation and communication.

2.1.5 “Development of an Algorithmic Approach for Hiding Sensitive Data and Recovery of Data based on Fingerprint Identification for Secure Cloud Storage”[5]

The paper presents a technique based on algorithms that uses encryption and fingerprint identification to secure sensitive data stored in cloud storage. The Triple Encryption Standard (3DES) cryptography algorithm and the MD5 (Message Digest) algorithm are combined in the proposed security model to offer the data multiple layers of protection. An extra degree of physical security is added by using fingerprint identification, which makes sure that only people with permission can access the data. In order to confirm the integrity of data stored in the cloud, the concept of remote data integrity auditing is also covered in this paper. Identity-based cryptography serves as the foundation for this suggested system, which has been proven to be effective and safe.

2.1.6 “Automated Biometric Authentication with Cloud Computing”[6]

This paper discusses the growing trend of individuals and organizations moving their data and services to cloud environments, and how this has led to a transfer of security control from data owners to cloud service providers. The difficulties in restricting authorized users' access to data in cloud environments and the drawbacks of conventional authentication techniques like security tokens and passwords are brought to light. In order to control access remotely in the cloud, the paper presents biometric-based authentication as a workable and trustworthy solution. It highlights the necessity of addressing privacy issues and making sure cloud service providers are not abusing biometric templates.

2.1.7 “Biometric Based User Authentication and Privacy Preserving In Cloud Environment”[7]

The two main issues addressed in this paper are data security and availability in cloud storage and data security during authorization. The significance of authorization by authorized delegates and data owners is frequently disregarded by current methods. The suggested system focuses on file security using the SHA algorithm and secure authorization through fingerprint analysis using the minutiae map algorithm. Additionally, it guarantees data availability across a number of cloud storage platforms, lowering the possibility of unavailability and offering storage that fits the customer's budget.

2.1.8 “A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing”[8]

In this paper biometric data undergoes encryption before being transmitted to the cloud database. To perform a biometric verification, the server owner encrypts inquiry data and submits it to the cloud. The cloud, in turn, conducts recognition tasks on the encrypted data and returns the results to the server owner. A comprehensive security assessment indicates that the proposed system maintains robust security even in the face of potential attacks attempting to mimic detection requests and collude with the cloud.Comparative evaluations with previous protocols demonstrate that the recommended strategy excels in both training and detection metrics. The experimental and novel findings affirm the enhanced performance of this approach, positioning it as a secure and efficient solution for the integration of biometric authentication with cloud-based storage and processing.

2.1.9 “BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud"[9]

The paper proposes BAMHealthCloud, a cloud-based healthcare data management system with biometric authentication to guarantee data security. The system tackles the security risks that the healthcare sector faces as a result of population growth and technological advancements. With its high accuracy for safe data access and retrieval, biometric authentication is suggested as an appropriate way to address the drawbacks of password forgetting and token theft in standard safety mechanisms.

2.1.10 “An Efficient Biometric Identification in Cloud Computing With Enhanced Privacy Security”[10]

In this paper, the idea of biometric identification is presented along with its significance in terms of reliability and convenience across a variety of applications.In order to protect biometric data, privacy-preserving measures are necessary, as this statement highlights. Existing matrix-transformation-based schemes are not sufficiently secure, and schemes based on homomorphic encryption suffer from low computational efficiency.The study proposes a new scheme that makes use of extra randomness and the characteristics of orthogonal matrices to improve security, and it also uncovers a known-plaintext attack vulnerability in a recently proposed matrix-transformation-based scheme.In addition to providing greater computational efficiency over comparable schemes, the suggested scheme is demonstrated to withstand attacks using both chosen and known plaintexts. Enhancing the privacy security of sensitive biometric data, it can support a large-scale database for practical biometric identification.

2.1.11 “Biometric Authentication for Cloud Service Provider in Multiple Cloud Storage System”[11]

This paper focuses on the use of the identity-based data outsourcing (IBDO) scheme in cloud storage services to provide auditing, controllable outsourcing, and integrity on outsourced files.With the help of their identities, approved entities are able to upload data on behalf of users through the IBDO scheme.The use of biometric authentication—more especially, fingerprint analysis—to improve system security is also introduced in this paper.The research suggests a split and merge method for a multiple cloud storage system, in which files are split into multiple fragments and stored in multiple locations, to mitigate security risks.

2.1.12 “Voiceprint-biometric template design and authentication based on cloud computing security”[12]

The paper provides a new approach that uses homomorphic encryption along with an authentication scheme to protect voiceprints and authenticate users in cloud computing environments.The suggested system ensures biometric security in an open network by enabling the measurement of voiceprint distortion without revealing the raw data.In order to facilitate queries and matching without having to decrypt the data, the client contributes encrypted voiceprint data to the system, preserving biometric security.If the security parameters are kept confidential, the voiceprint templates' diversity, cancelability, and irreversibility guarantee security.

2.2 Key Gaps in the Literature

2.2.1 The paper does not delve into the aspect of scalability, a critical consideration for cloud systems managing substantial user and data loads [1].

2.2.2 The investigation of the real-world performance and scalability of the proposed system in scenarios with a high user count is not comprehensively explored in this paper [2].

2.2.3 The potential limitations or drawbacks of the Privacy Preserving Steganography-based Biometric Authentication System (PPS-BAS) for cloud environments are not addressed in the paper [3].

2.2.4 A detailed analysis of the security vulnerabilities or potential attacks to which the proposed biometric authentication scheme may be susceptible is not provided in the paper [4].

2.2.5 The paper lacks a thorough discussion of the limitations of the proposed algorithmic approach for concealing sensitive data and recovering data based on fingerprint identification for secure cloud storage [5].

2.2.6 The shortcomings of the suggested method are not addressed in the paper; instead, the focus is primarily on issues, solutions, and privacy concerns surrounding biometric-based authentication in cloud computing [6].

2.2.7 The paper does not fully investigate the performance and effectiveness of the suggested identity-based data outsourcing technique [7].

2.2.8 In the event of cloud server downtime or cyber attacks, financial transactions relying on cloud-based biometric authentication could come to a standstill [8].

2.2.9 The paper does not discuss the scalability and feasibility of implementing the proposed system in a large-scale healthcare environment [9].

2.2.10 The scalability of the proposed scheme or its performance in handling a large number of biometric templates in a real-world scenario is not discussed in the paper [10].

2.2.11 The paper does not discuss the limitations of biometric authentication, including the likelihood of encountering false positives or false negatives [11].

2.2.12 The experimental results are based on a specific Mandarin continuous speech recognition training database, limiting the generalizability of the findings to other languages or speech recognition systems [12].

Table : 2.2.1 Literature Table

S.No.	**Paper Title[cite]**	**Journal/Conference (year)**	**Tools /Technologies/ Dataset**	**Results**	**Limitations**
1.	A Proposed Biometric Authentication Model to Improve Cloud Systems Security[1]	2022	MATLAB programming language	The proposed system performs the biometric authentication process securely and preserves the privacy of user information.	The paper does not provide information about the scalability of the proposed model, which is important for cloud systems that handle a large number of users and data.
2.	BAMCloud: a cloud based Mobile biometric authentication framework[2]	2022	Two sensors are used to input the data	Provide security solutions for mobile banking customers . The proposed framework is foolproof for fraud detection also, as the training data chosen for the proposed system has sufficient number of skilled forgery examples.	The paper does not provide a detailed analysis of the scalability and performance of the proposed system in real-world scenarios with a large number of users.
3.	Privacy preserving steganography based biometric authentication system for cloud computing environment[3]	2022	Multilevel DWT technique And continuous pigeon inspired optimizer (CPIO) algorithm,Q-learning technique	The proposed PPS-BAS for cloud environments showed enhanced outcomes compared to recent state-of-the-art biometric authentication systems.	The paper does not discuss the potential limitations or drawbacks of the proposed PPS-BAS for cloud environments

4.	Secure biometric authentication with deduplication on distributed cloud storage[4]	2021	Sensors, AWS cloud services	The most significant task carried out in this research work is biometric cryptographic security and reducing the de-duplication of data in cloud storage.And provide more reliability and fast encryption techniques	The paper does not provide a detailed analysis of the security vulnerabilities or potential attacks that the proposed biometric authentication scheme may be susceptible to.
5.	Development of an Algorithmic Approach for Hiding Sensitive Data and Recovery of Data based on Fingerprint Identification for Secure Cloud Storage [5]	2021	MD5, 3DES algorithms are used	The proposed algorithmic approach combines encryption algorithms, fingerprint identification, and remote data integrity auditing to enhance the security and privacy levels of cloud storage	The paper does not provide a detailed discussion on the limitations of the proposed algorithmic approach for hiding sensitive data and recovery of data based on fingerprint identification for secure cloud storage.
6.	Automated Biometric Authentication with Cloud Computing[6]	2021	Use of traditional encryption techniques such as AES or RSA for data encryption in the cloud environment	Biometric-based authentication can offer a practical and reliable option for remote access control in cloud environments	The paper focuses more on the challenges, solutions, and privacy concerns related to biometric-based authentication in cloud computing, rather than discussing the limitations of the proposed approach

7.	Biometric Based User Authentication and Privacy Preserving In Cloud Environment [7]	2021	Standard dataset images are used for fingerprint analysis.SHA algorithm ,Minutiae Map algorithm (MM	The paper proposes an identity-based data outsourcing technique for data security during authorization and storage in a cloud environment.	The paper does not provide a detailed analysis of the performance and efficiency of the proposed identity-based data outsourcing technique.
8.	A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing[8]	2020	Used sensors to capture the biometric data	Cloud-based biometric authentication offers several benefits for financial transactions, including enhanced security due to the difficulty of replicating biometric traits, convenience by eliminating the need to remember multiple passwords or PINs,	If the cloud server experiences downtime or faces cyber attacks, financial transactions relying on cloud-based biometric authentication could grind to a halt
9.	BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud[9]	2020	The signature samples were collected from 9000 users.	The use of this model ensures the scalability, flexibility, and robustness of the system. A speedup of 9x was achieved by BAMHealthCloud	The paper does not discuss the scalability and feasibility of implementing the proposed system in a large-scale healthcare environment.
10	An Efficient Biometric Identification in Cloud Computing With Enhanced Privacy Security [10]	2019	Homomorphic encryption, Matrix-transformation	The paper proposes a new privacy-preserving biometric identification scheme that utilizes the property of the orthogonal matrix and additional randomness to enhance security..	The paper does not discuss the scalability of the proposed scheme or its performance in handling a large number of biometric templates in a real-world scenario.

11	Biometric Authentication for Cloud Service Provider in Multiple Cloud Storage System [11]	2019	Identity-based data outsourcing (IBDO) technique is used	The paper proposes an identity-based data outsourcing (IBDO) scheme that allows designated entities to upload data on behalf of the user, providing integrity, controllable outsourcing, and auditing of outsourced files .	The limitations of using biometric authentication, such as the potential for false positives or false negatives, are not discussed in the paper.
12	Voiceprint-biometric template design and authentication based on cloud computing security [12]	2011	Codebook for voiceprint matching, Homomorphic Encryption	The paper proposed a novel voiceprint protection approach for cloud computing environments, utilizing homomorphic encryption and an authentication scheme. The system allows for distortion measurement of voiceprints without disclosing raw data, ensuring the security of biometrics in an open network .	The experimental results are based on a specific Mandarin continuous speech recognition training database, which may limit the generalizability of the findings to other languages or speech recognition systems.

Chapter 3: System Development

3.1 Requirements and Analysis

Functional Requirements:

Capturing User's Face: The primary step is to take photos of the users' faces. This is usually the process performed with a webcam or a camera. The users would have to be in front of the camera so that the faces can be seen clearly.

Storing Face Data: After the images are snapped, the system has to keep this information. The camera records the images of the user's faces and also some relevant information about each user, such as their name or ID. The information that is obtained is the one that the system will utilize in the future to identify the users' faces.

Training the System: The system has to be trained to recognize the faces of the users after gathering the face data. This signifies the process of transforming the faces in the images to remove the features that are common to each person. The system, in turn, discovers that the features which started with the user information are related to the users.

Verification and Feedback: The enrollment process is a time that requires the input of the users which is to give the feedback. Such a thing could be realised by showing them their captured images and asking them to verify if they're correct. In case of problems or mistakes, the people should be allowed to retake the pictures.

Testing and Validation: After the enrollment procedure is finished, it is essential to check the system to ascertain that it can definitely identify the users who have been enrolled and their faces. The above may cash out to be phony or fake world occurrence like the trustworthiness of the system in real life.

Optimization: In conclusion, the enrollment procedure should be revisited taking into account user feedback and system performance. The process of producing a high resolution image could be improved by either making the image capturing process better, making the training algorithms better, or by making some changes to the user interface to make the process smoother and more efficient.

Non-Functional Requirements:

Performance:

- **Real-time Processing:** The system, therefore, should be able to carry out face detection and recognition tasks in the real-time mode for the purpose of timely attendance tracking.

- **Scalability:** The system should be able to deal with the loads, for example, it should be able to accept a large number of users and at the same time, at the same time, attendance requests and not drop the performance.

- **Throughput:** The system should be able to deal with high throughput, that is, it should handle several face detection and recognition requests at the same time at the same time.

Reliability:

- **Availability:** The system should be extremely available, with the very limited downtime to make sure the attendance tracking function is always working.

- **Fault Tolerance:** The system should be very robust to failures, having built-in mechanisms to recover from the errors and retain the functionality.

- **Error Handling:** The system should inform the users through the error messages and should deal with the exceptions in a smooth way to lessen the disturbance of the users

Security:

- **Data Privacy:** The system is supposed to maintain the confidentiality and privacy of biometric data, following the privacy laws and the industry best practices.

- **Authentication:** The system should have secure authentication methods to prevent unauthorized usage and guarantee that only authorized users can access attendance data.

- **Integrity:** Attendance data should be safeguarded from manipulation or unauthorized changes to maintain its validity and trustworthiness.

Usability:

- **User Interface:** The system must be of an easy to use and intuitive design so that users can easily start the attendance tracking, check the attendance records and do other things.

- **Accessibility:** The system should be available to the users with disabilities, checking the accessibility standards and guidelines to ensure the inclusivity.

- **Performance Feedback:** The system should provide feedback to the users when they are in face detection and recognition processes so that they can be aware of the system's status and progress.

Scalability:

- **Capacity Planning:** The system should be made in a way that it can grow and scale in the future and should have the provisions for the expansion of the capacity as per the requirement.

- **Resource Utilization:** The system should maximize resource usage, thus, the memory and CPU usage will be reduced and the operation on different hardware will be efficient.

Maintainability:

- **Modularity:** The system should be the modular and the well-structured, thus, it is easy to maintain and the future enhancements can be easily done.

- **Documentation:** A complete documentation should be given, for instance, system architecture, code comments, and user manuals which will help the system maintenance and the knowledge transfer.

Compatibility:

- **Platform Compatibility:** The system has to be compatible with various operating systems and hardware configurations so that it can be widely used and its deployment is flexible.

- **Integration:** The system should be able to support the integration with other software systems and APIs thus, the data exchange and the interoperability will be seamless.

Regulatory Compliance:

- **Legal Compliance:** The system should abide by the applicable laws, regulations, and standards that are related to the collection, storage, and processing of biometric data, which include GDPR, HIPAA, and CCPA.

- **Ethical Considerations:** The system should be based on ethical principles and guidelines, which would mean the protection of the biometric data and the respect for the users' privacy and their consent.

Analysis: Here is the breakdown of the analysis process:

Architecture:

- **Data Collection:** The face recognition system is a device that captures images or video frames with faces that are taken from the webcam or camera. These photos are the ones that are used as the input for the face detection and recognition process.

- **Face Detection:** The face detection module is able to detect and find the human faces in the images or frames that are captured. OpenCV has the pre-trained face detection models like Haar cascades or deep learning-based models. Detected faces are usually highlighted by bounding boxes.

- **Preprocessing:** The faces detected before doing the face recognition may be subject to the preprocessing steps, which, in turn, can improve their quality and normalize them for better recognition accuracy. Preprocessing may comprise of procedures like resizing, grayscale conversion, histogram equalization, or face alignment.

- **Feature Extraction:** The following step is about the extraction of the facial features from the preprocessed face images. Features could be the geometric measurements of facial landmarks (like eyes, nose, and mouth) or deep learning models could learn to extract the representations from them. These attributes are the special features that are the unique identity of each person's face.

- **Face Recognition:** The face recognition module matches the facial features that were extracted with the features of the people that are in the database. Multiple algorithms are available for face recognition.The system compares the input face with the faces in the database and finds the best match(es).

- **Attendance Tracking:** After a face is caught, the system notes the attendance of the person whose face it is. This may mean that the system needs to be updated with the attendance status (e.g. present or absent) of the students. g. Therefore, the selected status (present/absent) together with the extra details such as timestamps and user IDs.

- **User Interface:** An interface component enables users to connect with the system through its interface. This may be a GUI where users can initiate the attendance process, look at the attendance reports, and do the administrative tasks like adding or removing users from the system.

Data Flow:

- **Enrollment Process:** The device should be used to capture facial features through its camera.Create a facial template for subsequent process and storage, making sure it bears the owner's identity.
- **Authentication Process:** Collect authentic facial landmarks in an attempt to authenticate logins. Use face-api.js to compare the captured traits to the stored samples.

User Interface:

- **Enrollment UI:** Facilitate face recognition in user-friendly environment through enrollment. Provide directions that are easily understandable by users.

- **Authentication UI:** Build a user-friendly front-end for immediate face identification while logging in. Provide information to the users regarding the authentications' success or failures.

- **Real-time Processing:** Enhance react components and face-Api.js configuration for real time implementation. Use of asynchronous processing could help in avoiding UIs freeze ups
- **Caching and Local Storage:** Use local cache of enrolled templates for better speed in authentication. Provide appropriate security for locally stored data.

Security Measures:

- **Encryption:** Encode face templates before storing and transmitting them. Ensure continued review and revision of your encryption protocols.

- **Spoofing Prevention:** Create strategies to counter the most prevalent techniques of spoofing including phishing, impersonation through use of photos and videos.

- **Regular Update and Patch Management:** Maintain the system components, comprising of Python libraries, OpenCV, and the operating system dependencies, with the most recent security patches and updates. Keep on checking for security vulnerabilities and apply the patches as soon as the problems are found to reduce the risks of the threats.

- **Security Training and Awareness:** Offer security training and awareness programs for system administrators, operators, and end-users. Teach the users about the security best practices that include choosing strong passwords, being able to recognize phishing attempts, and reporting the suspicious activities.

3.2 Project Design and Architecture

Project Design: Algorithm:

- Start
- User Initiates Authentication
- Capture Biometric Data (e.g. face by using cam roll)
- Enroll or Compare Biometric Data
- Enrollment not done Then First enroll and then the user will be registered And follow the further steps.
- Biometric Data Not Found in Database then Authentication Failed
- Biometric Data Found in Database then Authentication Successful And Access will be Granted
- End

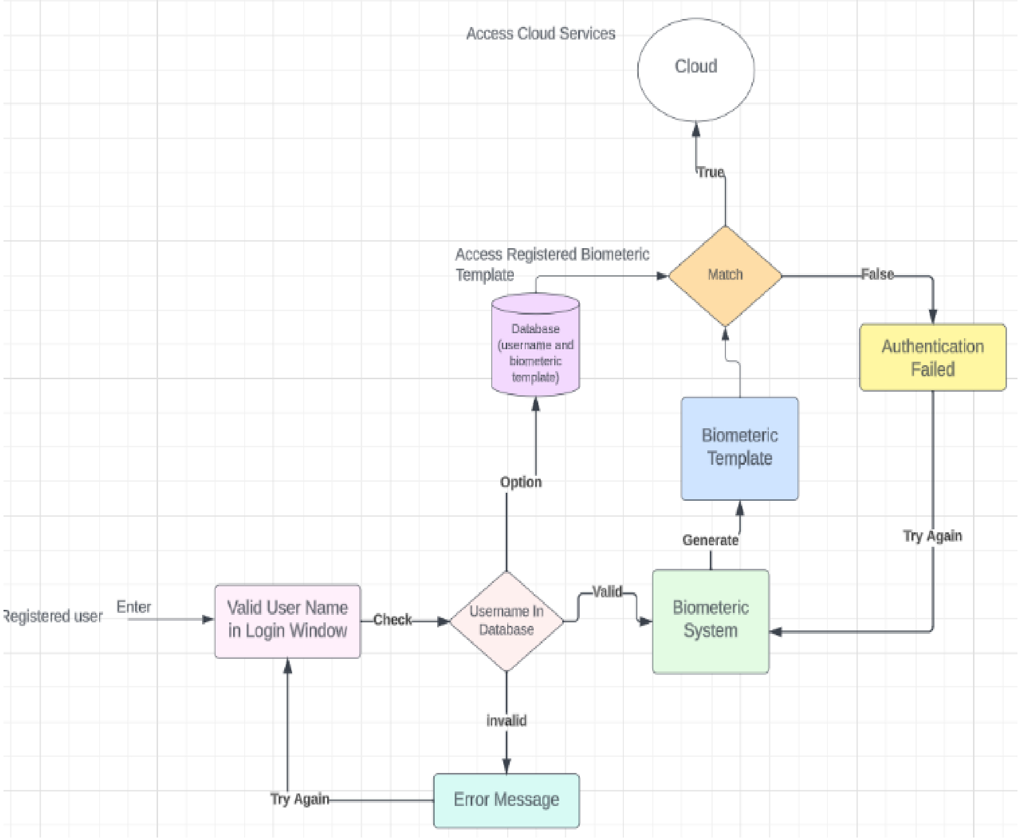


Figure 3.1: Project Design

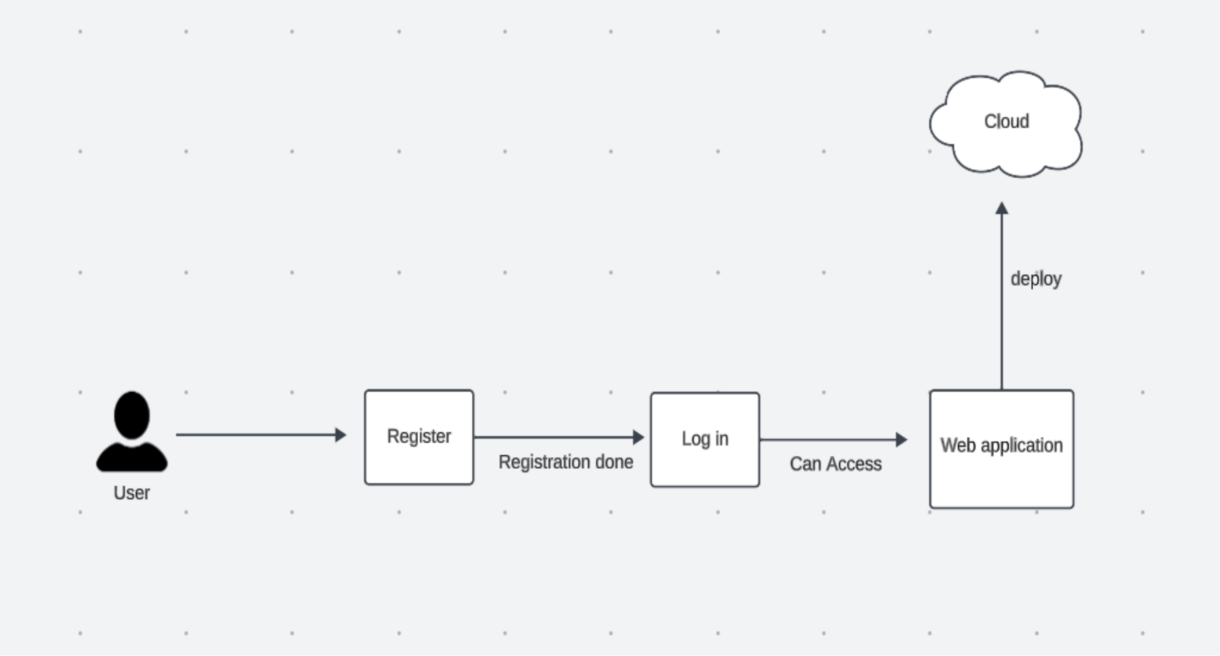


Figure 3.2: Project Workflow

User Interface: Design a user interface that will allow the user to communicate with the system. This could be a GUI that is implemented using the libraries such as Tkinter or a web-based interface that is developed with the help of the frameworks like Flask or Django. There should be possibilities for the beginning of the attendance process, the attendance reports viewing, the addition or the removal of the users and the settings of the system.

Face Detection Module:

Introduce a face detection module using OpenCV that is capable of detecting faces in images or video streams that are either captured by a webcam or a camera. Pick a face detection algorithm, for instance, Haar cascades or deep learning-based models

Face Recognition Module:

Create a face recognition module to recognize individuals according to their facial features. Pick a face recognition algorithm .The recognition model must be trained on a dataset of labeled face images to learn the unique facial features of each person.

Attendance Tracking: Develop the ability to track attendance through the detection of faces that are already recognized. Keep attendance records in the database which contains timestamps and attendance status (e. g. present or absent). g. , present/absent). The application of the logic to mark users as present when their faces are detected during the attendance process is essential.

User Enrollment: Let us come up with a system of enrolling new users in the system. The pictures of the faces of the users are to be taken and stored in the database together with their names or IDs. The face recognition model is to be trained with the enrolled users' facial images so that it will be able to recognize the users during the attendance tracking.

Security Measures: Security measures are to be put into place to safeguard the sensitive information and stop the access by unauthorized persons. There are features like data encryption, access control, anti-spoofing measures, and secure communication protocols that should be included.

Error Handling and Logging: Set up mechanisms to deal with errors and unexpected situations in a nice manner. Log system events, errors, and user activities for debugging, auditing, and monitoring purpose.

Testing and Validation: Check the system thoroughly to make sure the system is working properly, accurately, and reliably. Check whether the system is working well under different lighting conditions, angles, and environmental factors. Find out the views of the users and stakeholders which will help to identify the areas for improvement.

Deployment and Integration: Choose the place, where the system will be used, for example, classrooms, offices, or organizational settings. Merge the system with the existing infrastructure, hardware, and software elements that are required. Cut the red tape and provide the training and the documentation that are necessary to make the system work.

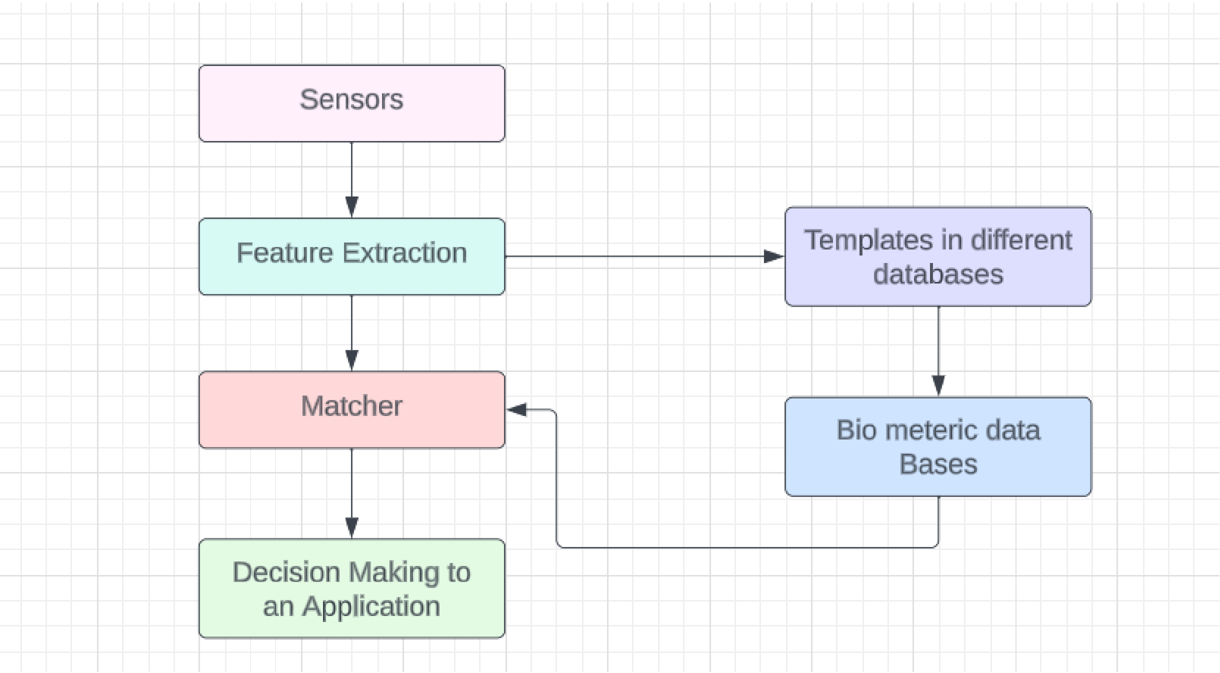

Sensors
Feature Extraction
Templates in different databases
Matcher
Bio meteric data Bases
Decision Making to an Application

Figure 3.3 : Flow diagram for the further execution of web app

3.3 Data Preparation

- **Data Collection:** Collect a set of images of faces of the people who will be included in the attendance system. Make sure that the dataset has a wide range of individuals, reflecting the differences in lighting conditions, facial expressions, angles, and occlusions. Use a webcam or camera to capture pictures of people's faces in different surroundings (e. g. indoors, outdoors).

- **Image Preprocessing:**The collected images should be preprocessed to improve their quality and normalize them to increase the recognition accuracy. Make images grayscale to simplify processing and cut down the computational load. The images can be changed to a standard size to make the dataset uniform and to boost the model efficiency.Histogram equalization is a technique that helps to increase the contrast and thus the visibility of facial features.

- **Face Detection and Cropping:** Apply OpenCV's face detection algorithms to find and take out faces from the preprocessed images. Implement a face detection algorithm (e. g. deep learning) in order to recognize the face. g. , Haar cascades, deep learning-based models) to identify areas of interest that contain faces. Remove the detected faces from the original images to make a dataset of face images for each person.

- **Labeling and Organization:** Give every person in the dataset a unique label or identifier. Arrange the dataset into separate folders or directories, each one representing a different person and containing his face images. Formulate a link between the labels and the names or IDs of the individuals for the training and recognition purposes.

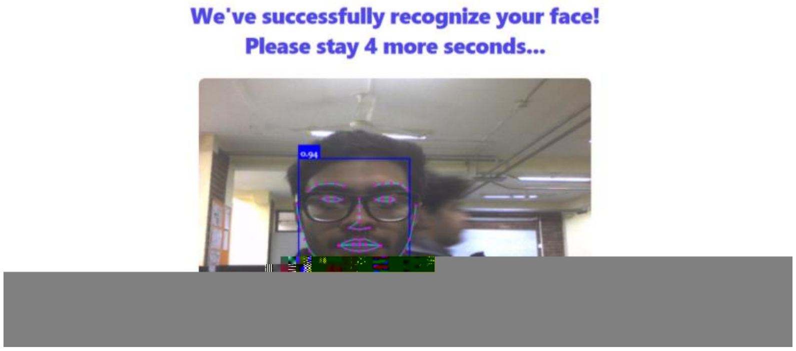
- **Labeling and Organization:** Give each person a separate label or an identifier to the dataset. Create the dataset into the separate directories or folders, each folder representing a different person and having its face images. Establish a connection between the labels and the names or IDs of the individuals used as references during the training and recognition phases.

- **Data Augmentation :** Enhance the dataset with the changes of the original images to the variation and, hence, the model generalization will be improved. Implement the transformations that include rotation, translation, scaling, flipping, and randomizing to get more training samples.

- **Data Splitting:** The dataset is divided into the training and the validation sets in order to evaluate the model's performance and prevent overfitting. Allocate a part of the dataset for validation and check the performance of the model on the unseen data.

- **Training Data Preparation:** The training data should be created by loading the face images and their labels into memory. The images and labels have to be converted into the suitable data structures (e. g. dictionaries, lists) the machine learning frameworks or libraries you will use for training will be compatible with the NumPy arrays, lists, etc.

- **Enrollment Data Preparation:** Gather the enrollment data by taking the images of the individuals' faces and saving them together with their names or IDs in a database. Get the face from the enrollment images and turn them into reference templates for face recognition during attendance tracking.



We've successfully recognize your face!
Please stay 4 more seconds...

Fig 3.3.1 Data Collection

2.Now the data will be stored in website and will recognize the user and help user to login to have access to the cloud .And now registered user can have the access to the web application

3.4 Implementation :

The goal of using React and face-api.js to implement a facial recognition-based authentication project is to seamlessly integrate state-of-the-art facial recognition capabilities into a safe and user-friendly interface. With the help of React, the project creates an easy-to-use interface and incorporates webcam access for instantaneous facial image capture, all while guaranteeing a seamless user experience. The face-api.js-powered core functionality prioritizes precise face detection and recognition by identifying distinct facial features for safe authentication. User biometric data is protected by strict measures, emphasizing the importance of privacy and data handling. Real-time user feedback during authentication is given top priority in this project, which helps users navigate the process and gracefully handles any errors. Iterative development using user interactions is part of the continuous improvement cycle, which helps to improve the facial recognition model. Strong encryption, access controls, and frequent updates to minimize potential vulnerabilities all continue to be top priorities when it comes to security. At every stage of implementation, comprehensive testing guarantees the project's accuracy, security, and general quality.

- **Setup Environment:** Install Python and the libraries that are necessary like OpenCV, NumPy, and any extra dependencies. The connection and access to the camera or webcam should be checked to make sure that the images can be captured.

- **Face Detection:** Apply the face detection module using OpenCV's pre-trained Haar cascades or deep learning-based face detector models. The face detection module will be used to detect faces in real-time video streams or images from the webcam.

- **Face Recognition:** Create a face recognition model based on a dataset of face images that are labeled. A facial recognition module can be created through the use of algorithms such as Eigenfaces, Fisherfaces, LBPH, or deep learning-based methods (e. g. The artificial intelligence applications include CNN (Convolutional Neural Networks, Siamese Networks, FaceNet). The trained model is loaded and then used to recognize faces in the detected regions.

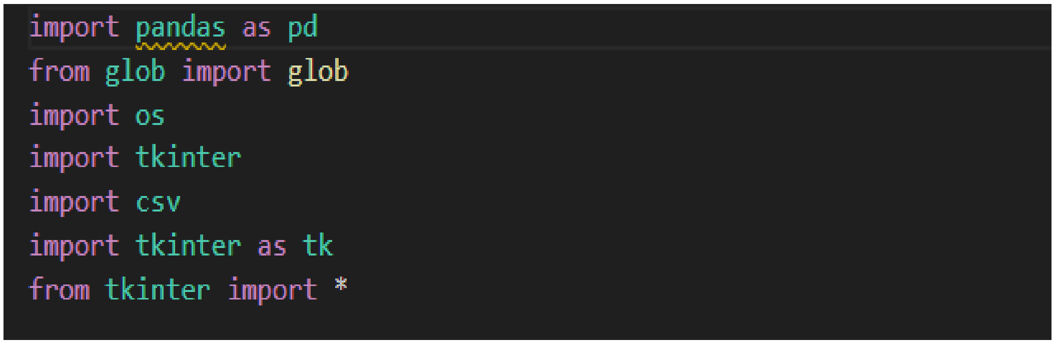
- **Attendance Tracking:** After a successful face recognition, log attendance by the date and time of the recording and the name or ID of the identified person. The records of store attendance are to be stored in a database or log file for later analysis and reporting.

- **User Interface:** Stage a user interface (UI) development for the attendance system. The page should have the choices for the commencement of the attendance process, the attendance reports, the addition or the elimination of users, and the settings of the system. Create the UI using the GUI libraries such as Tkinter, PyQt, or web frameworks like Flask or Django.

- **Integration and Testing:** The face detection, recognition, and attendance tracking modules should be incorporated into a system that is unified and works together. Create extensive tests of the system to make sure that the system works, the results are accurate and the system is reliable. Test the system in different lighting conditions, angles, and environmental factors to establish its performance.

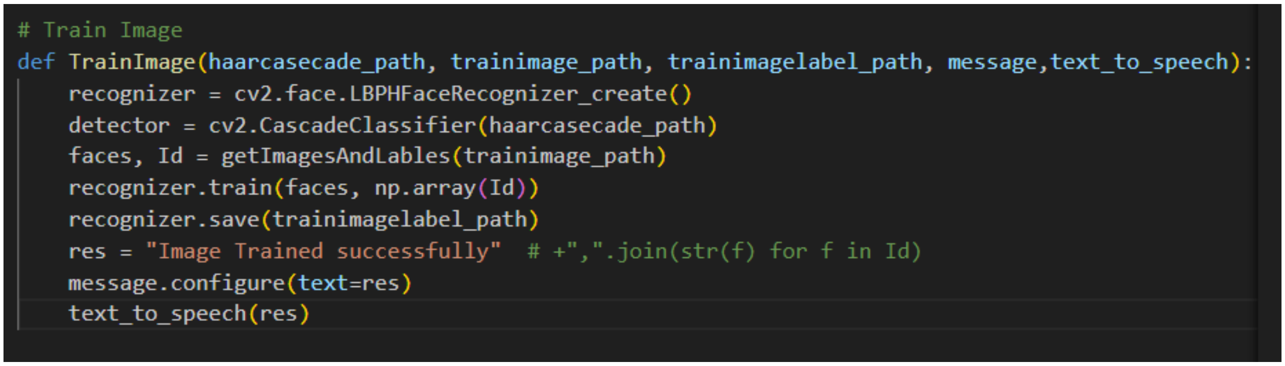
- **Security and Privacy**: Make sure to put in place security systems to guard sensitive information and to stop the unwanted access. The features such as data encryption, access control, anti-spoofing measures, and secure communication protocols should be in addition to them. Lock yourself in the privacy law and make sure you get the user's approval before collecting and processing facial data.

- **Deployment and Usage:** The system will be deployed in the desired environment, which could be the classrooms, the offices, or the organizational settings. Give the documentations and user training and therefore for deployment and adoption. Consulting the users and stakeholders for getting their opinions on the implementation of the project will help in identifying the areas for improvement and then the implementation will be changed accordingly.



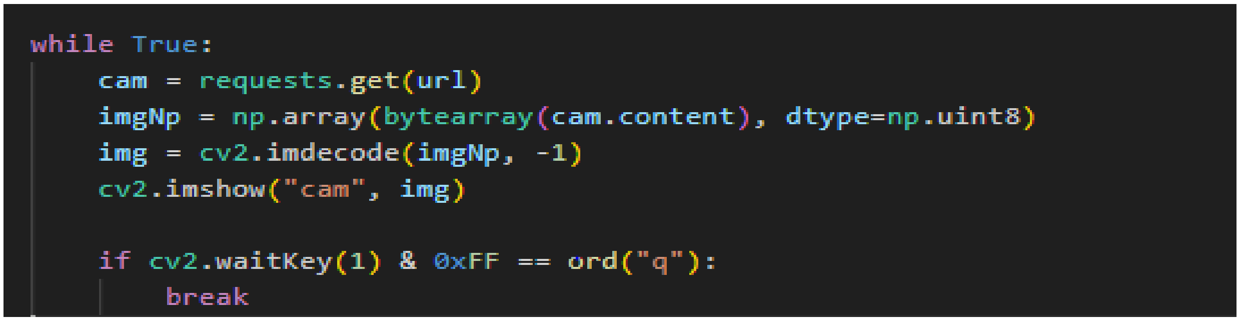
```
import pandas as pd
from glob import glob
import os
import tkinter
import csv
import tkinter as tk
from tkinter import *
```

Fig 3.4.1 Importing Libraries



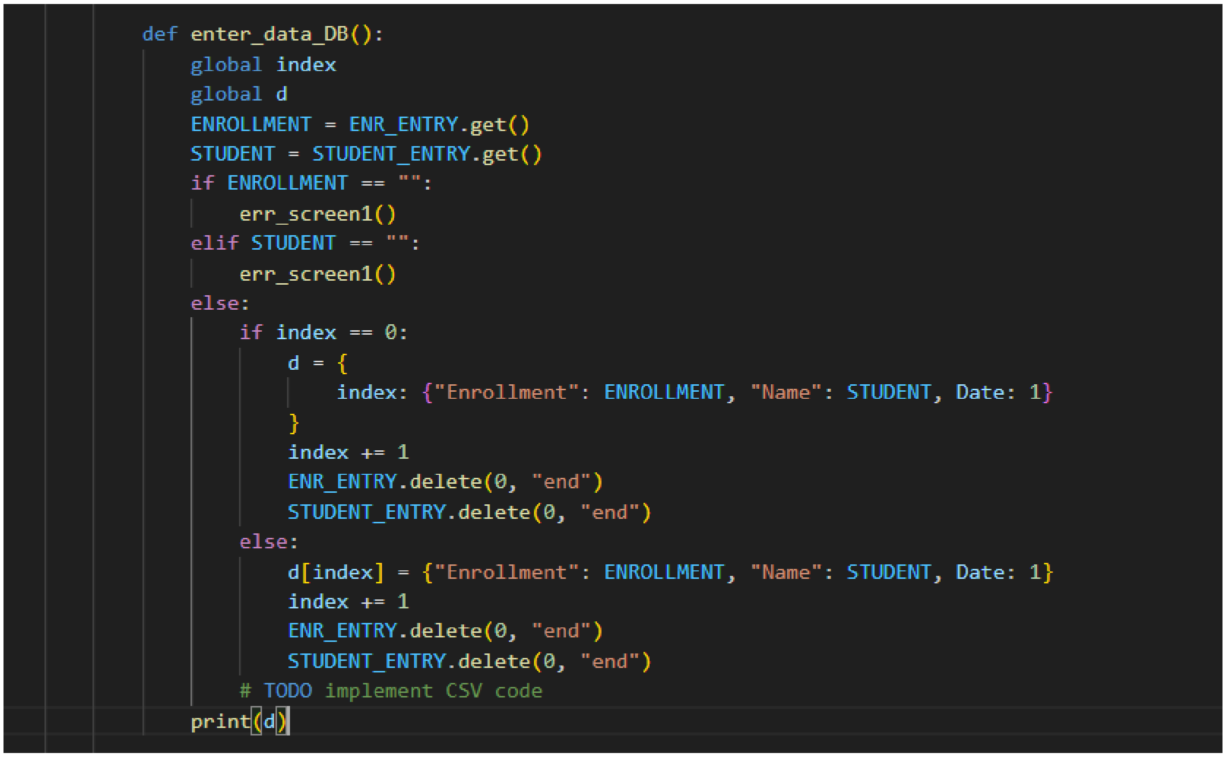
```
# Train Image
def TrainImage(haarcasecade_path, trainimage_path, trainimagelabel_path, message,text_to_speech):
    recognizer = cv2.face.LBPHFaceRecognizer_create()
    detector = cv2.CascadeClassifier(haarcasecade_path)
    faces, Id = getImagesAndLables(trainimage_path)
    recognizer.train(faces, np.array(Id))
    recognizer.save(trainimagelabel_path)
    res = "Image Trained successfully"  # +",".join(str(f) for f in Id)
    message.configure(text=res)
    text_to_speech(res)
```

Fig . 3.4.2 training image



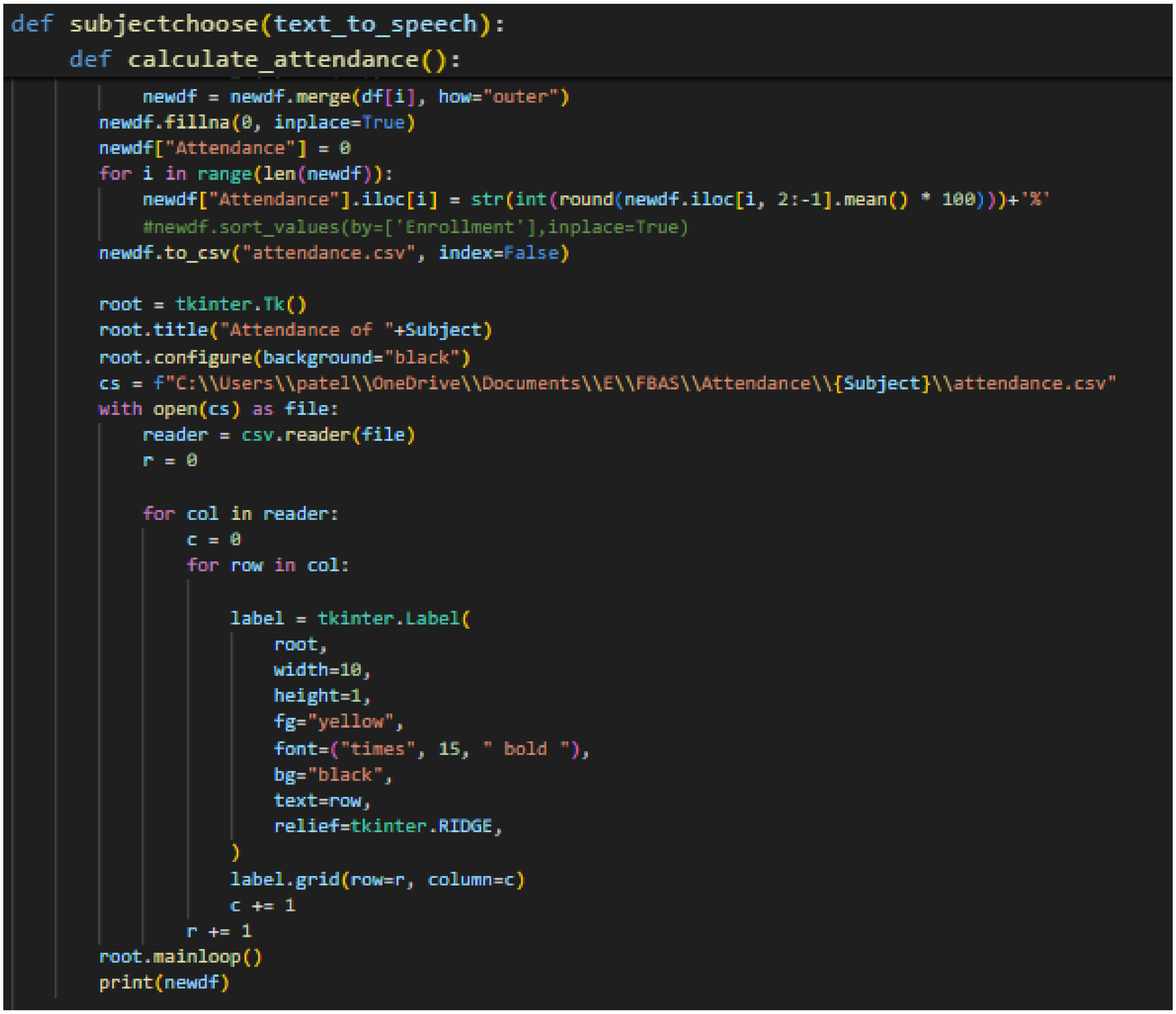
```
while True:
    cam = requests.get(url)
    imgNp = np.array(bytearray(cam.content), dtype=np.uint8)
    img = cv2.imdecode(imgNp, -1)
    cv2.imshow("cam", img)

    if cv2.waitKey(1) & 0xFF == ord("q"):
        break
```

Fig 3.4.3 capture frames from a video stream



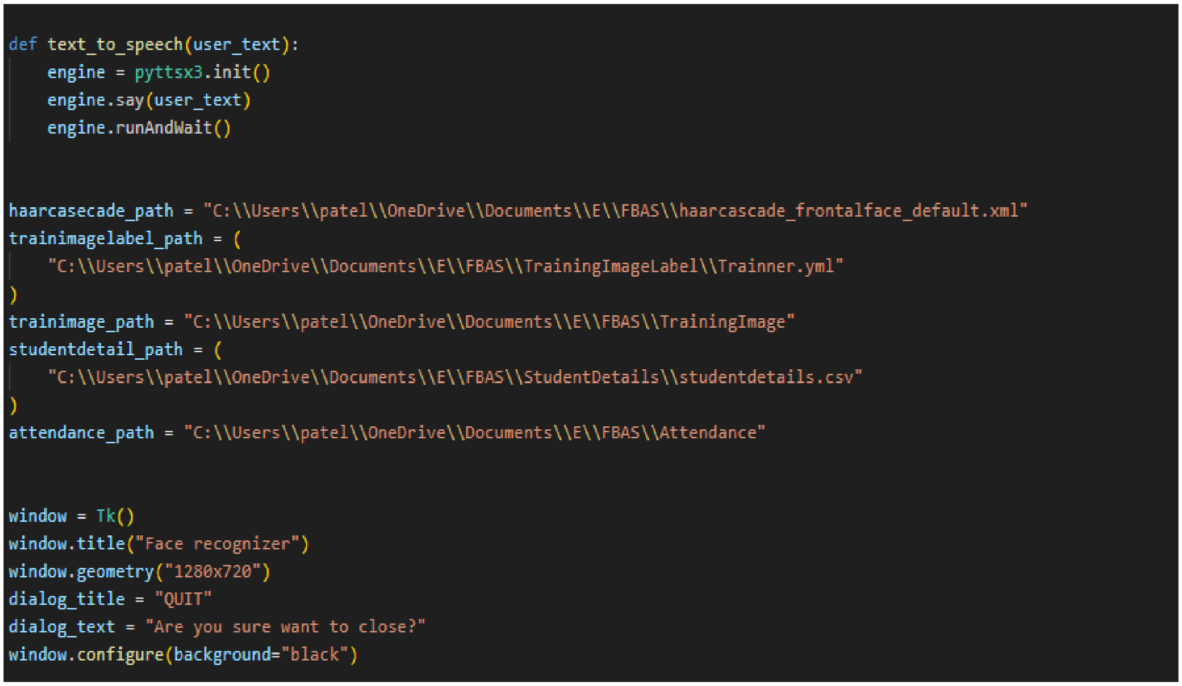
```
        def enter_data_DB():
            global index
            global d
            ENROLLMENT = ENR_ENTRY.get()
            STUDENT = STUDENT_ENTRY.get()
            if ENROLLMENT == "":
                err_screen1()
            elif STUDENT == "":
                err_screen1()
            else:
                if index == 0:
                    d = {
                        index: {"Enrollment": ENROLLMENT, "Name": STUDENT, Date: 1}
                    }
                    index += 1
                    ENR_ENTRY.delete(0, "end")
                    STUDENT_ENTRY.delete(0, "end")
                else:
                    d[index] = {"Enrollment": ENROLLMENT, "Name": STUDENT, Date: 1}
                    index += 1
                    ENR_ENTRY.delete(0, "end")
                    STUDENT_ENTRY.delete(0, "end")
                # TODO implement CSV code
            print(d)
```

Fig . 3.4.4 entering student data into a database



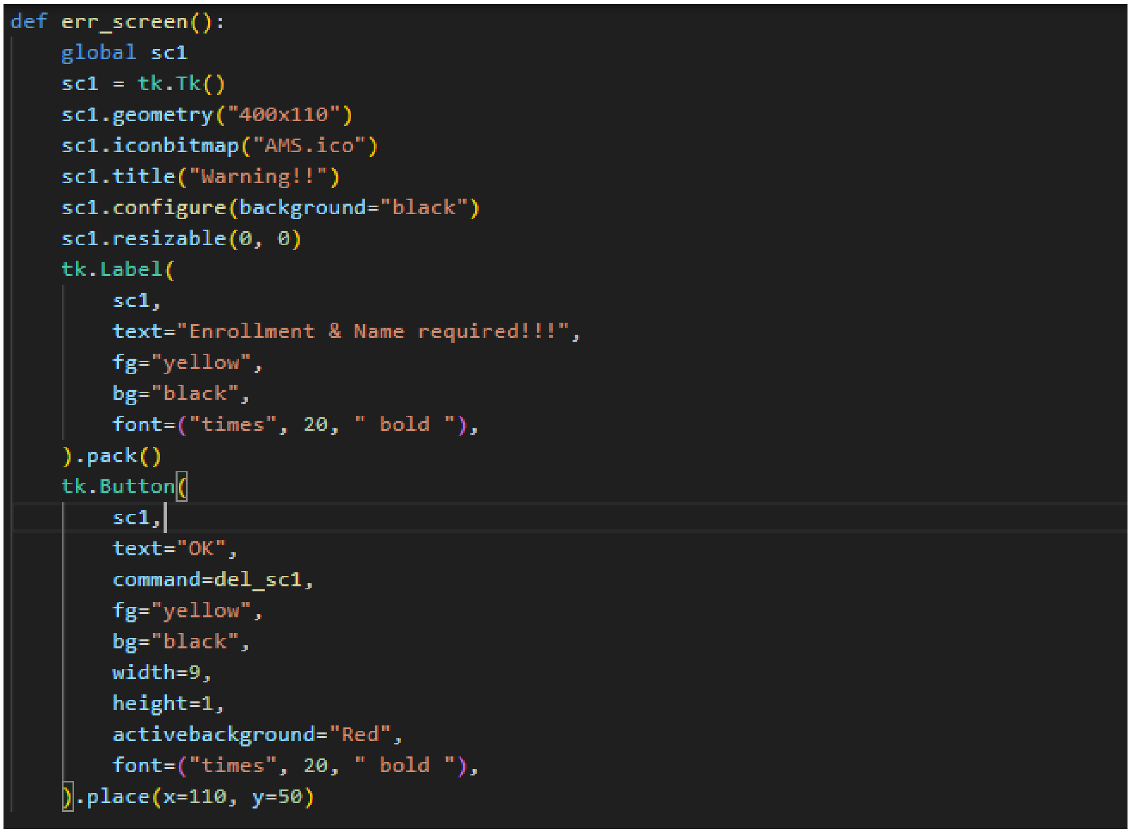
```python
def subjectchoose(text_to_speech):
    def calculate_attendance():
            newdf = newdf.merge(df[i], how="outer")
        newdf.fillna(0, inplace=True)
        newdf["Attendance"] = 0
        for i in range(len(newdf)):
            newdf["Attendance"].iloc[i] = str(int(round(newdf.iloc[i, 2:-1].mean() * 100)))+'%'
            #newdf.sort_values(by=['Enrollment'],inplace=True)
        newdf.to_csv("attendance.csv", index=False)

        root = tkinter.Tk()
        root.title("Attendance of "+Subject)
        root.configure(background="black")
        cs = f"C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\Attendance\\{Subject}\\attendance.csv"
        with open(cs) as file:
            reader = csv.reader(file)
            r = 0

            for col in reader:
                c = 0
                for row in col:

                    label = tkinter.Label(
                        root,
                        width=10,
                        height=1,
                        fg="yellow",
                        font=("times", 15, " bold "),
                        bg="black",
                        text=row,
                        relief=tkinter.RIDGE,
                    )
                    label.grid(row=r, column=c)
                    c += 1
                r += 1
        root.mainloop()
        print(newdf)
```

Fig 3.4.5 calculates attendance percentages for students



```
def text_to_speech(user_text):
    engine = pyttsx3.init()
    engine.say(user_text)
    engine.runAndWait()


haarcasecade_path = "C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\haarcascade_frontalface_default.xml"
trainimagelabel_path = (
    "C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\TrainingImageLabel\\Trainner.yml"
)
trainimage_path = "C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\TrainingImage"
studentdetail_path = (
    "C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\StudentDetails\\studentdetails.csv"
)
attendance_path = "C:\\Users\\patel\\OneDrive\\Documents\\E\\FBAS\\Attendance"


window = Tk()
window.title("Face recognizer")
window.geometry("1280x720")
dialog_title = "QUIT"
dialog_text = "Are you sure want to close?"
window.configure(background="black")
```

Fig.3.4.6 graphical user interface (GUI) window using the Tkinter library for a face recognition



```
def err_screen():
    global sc1
    sc1 = tk.Tk()
    sc1.geometry("400x110")
    sc1.iconbitmap("AMS.ico")
    sc1.title("Warning!!")
    sc1.configure(background="black")
    sc1.resizable(0, 0)
    tk.Label(
        sc1,
        text="Enrollment & Name required!!!",
        fg="yellow",
        bg="black",
        font=("times", 20, " bold "),
    ).pack()
    tk.Button(
        sc1,
        text="OK",
        command=del_sc1,
        fg="yellow",
        bg="black",
        width=9,
        height=1,
        activebackground="Red",
        font=("times", 20, " bold "),
    ).place(x=110, y=50)
```

Fig 3.4.7 Error message or warning generated

3.5 Key Challenges

As we are implementing the project step by step but some certain problems occurred during the development phase. The system in not detecting the user face even when getting registered so we used face-api.js library And which fully solved our problem . Complying to regulatory requirements for data privacy and security meant putting strict access controls and encryption methods into practice with care. Taking on these challenges required teamwork in identifying and resolving issues as well as a dedication to ongoing improvement. The final implementation has improved considerably as a result of this iterative process, guaranteeing a stronger and more flexible system.

Accurate Face Recognition: Consider attempting to identify a person's face in a picture where they may be standing in a different light, displaying distinct facial expressions, or perhaps donning sunglasses. It's challenging to make sure the system can consistently handle each of thesescenarios.

Gathering Good Images: You need a ton of images of various people taken from various perspectives and environments in order to train the system to identify faces. Obtaining these images and ensuring that they are sufficiently varied and clear can be difficult tasks.

Optimizing System Performance: Suppose that if you wanted to use the system, it took an eternity to think of anything? It must operate swiftly and with minimal computing resources consumed.

Respecting Privacy: People, particularly those who are at work or school, may not want their faces to be constantly scanned. We must guarantee that the system abides by the regulations on the gathering and use of personal data and respects individuals' right to privacy.

Maintaining Security: Just as you would want a lock on your door to keep out intruders, we must ensure that our system is impervious to attempts to trick it using a mask or photo.

Integrating with Everything : Image attempting to assemble a fresh puzzle piece into a completed one. It is imperative that we ensure our system is compatible with the other tools and systems that users are currently using.

Ensuring Usability: Recall how perplexing it was the first time you used a new software or gadget! It is imperative that we ensure our system is simple enough for folks to learn and utilize.

Increasing with Demand: Consider a scenario in which a restaurant, with a limited number of chairs, unexpectedly becomes extremely popular. Our system must be able to support large numbers of users without experiencing any hiccups or errors.

Bias and Fairness: Face recognition systems, in their function, may practice biases which cause inaccuracies or unjust treatment, especially in certain demographic groups. The issue of fairness and bias in AI systems is extremely challenging and it includes approach selection in dataset structuring, algorithmic design, and continuous checking the existing inequalities.

Robustness to Environmental Factors: One of the main aspects of face-recognition, which is related to the environment, is that the faces can be different due to weather conditions (e. g. rain or sun), background clutter (houses or vegetation) and camera quality. Creation of such adaptation to the future weather changes is significant for assurance of precision and accuracy in real-life contexts.

Cross-Domain Generalization: Face recognition models trained with pre-defined data might lose their ability to generalize if they are not used in the uncharted territories or conditions. Meeting the purpose of being optimally applied in different domains entails domain adaptation and transfer learning techniques.

Ethical Use and Accountability: Privacy risks arise with face recognition technology where there are concerns regarding surveillance, profiling and potentially, abuse of the technology as well. Articulating the ethical use, providing transparency, and using both accountability and oversight mechanisms for good usage are the cardinal points of responsible usage.

Chapter 4: Testing

4.1 Testing Strategy

Testing Strategy:

- **Unit Testing:** The first step in the systematic testing of a system is to check the individual components or units of the system separately to make sure that they are working correctly. Unit tests should be written for the modules with responsibilities for face detection, recognition, attendance tracking, and user interface functionalities. Utilize testing frameworks like unit test or py test to carry out the unit tests and run them on a frequent basis during the development process.

- **Integration Testing:** Check the interaction and the smooth working of the different modules or components of the system. Check that modules correctly exchange data and that their interactions will give the desired results. Carry out integration tests for cases such as face detection followed by face recognition, attendance logging, and user interface interactions.

- **End-to-End Testing:** Conduct the full system trial to check its actual behavior and functionality in real-life situations. The process of making the system like a real device of usage including starting the attendance process, enrolling users, recognizing faces and logging attendance is simulated. Deploy the end-to-end testing frameworks or scripts to automate the test scenarios and the system's performance and reliability evaluation is done.

- **Regression Testing:** Carry out the regression tests to check whether the latest changes or the updates to the system have caused the appearance of new bugs or the regressions. Redo the same test cases after making changes and confirm that the system reacts in the same way and as expected before. The use of version control systems to track the changes and to make the regression testing easier by the comparison of the current and the previous versions of the codebase is good.

- **Performance Testing:** The system is tested under different conditions, such as the number of users, lighting conditions and image resolution. Look at how fast the system responds, how much data it processes per second, and how much resources it uses to pinpoint the possible hindrances and improve its performance. Take advantage of the performance testing tools and the testing frameworks to create the load, stress, and scalability scenarios and to check the system's behavior under heavy usage.

- **Security Testing:** The system should be tested to find out its vulnerable parts and weaknesses that could put the security and privacy at risk. Penetration testing is the process of identifying the weak points of a computer system in a bid to obtain unauthorized access, which will help in detecting data breaches and spoofing attacks. The security measures that are to be implemented are the encryption, access control, and anti-spoofing measures. The effectiveness of these measures is to be evaluated through the testing.

- **User Acceptance Testing (UAT):** Take a step further and incorporate the end-users or stakeholders in the testing process of the system to confirm if it is fulfilling their needs and their expectations. Collection of user feedback on usability, functionality, and overall satisfaction with the system is essential. User feedback is a great tool to be used for the alteration and improvement of the actual implementation that takes on the user needs and preferences.

Testing Tools:

Unit Testing:

- **unittest:** Python's built-in unit testing framework, which presents a straightforward and scalable method to write and run unit tests for the separate components or units of the system.
- **pytest**: An acclaimed third-party testing framework for Python which has features such as fixtures, parameterized testing, and simple integration with other testing tools is a python-testing framework that is widely used by developers.

Integration Testing:

- **unittest:** Although mainly used for unit testing, unittest can also be used to write integration tests for testing the inter-module or component interactions of the system.
- **pytest:** Also, the same goes for pytest that can be used for integration testing by writing test cases that are supposed to test the interaction of the system with multiple components or functionalities.

End-to-End Testing:

- **Selenium:** One of the most common tools for the automation of web browser actions, Selenium is the right tool for the end-to-end testing of the web-based user interfaces in the face-to-face attendance system.
- **PyAutoGUI:** PyAutoGUI is a Python library that is cross-platform for GUI automation that can be used to simulate the user's interactions with the system's graphical user interface (GUI) components.

Regression Testing:

- **pytest:** Both unittest and pytest embrace regression testing through the possibility of running the existing test cases to make sure there are no new bugs or regressions after the changes or updates to the system.
- **Git:** The version control systems such as Git can be used to keep a track of all the changes made in the codebase and at the same time, they can be of great help in the regression testing by comparing the different versions of the code.

Performance Testing:

- **Locust:** A free-to-use load testing tool that operates in Python, Locust enables you to emulate thousands of users at once and thus you can evaluate the system's performance under load.
- **JMeter:** Apache JMeter, a widely used Java-based performance testing tool, is for load testing, stress testing, and performance monitoring of web-based applications.

Security Testing:

- **OWASP ZAP (Zed Attack Proxy):** The OWASP ZAP, which is a web application security testing tool, can be used to detect and eliminate the security vulnerabilities in the web-based components of the face-based attendance system.
- **Nmap:** A network scanning tool that is employed to find the hosts and services of a network and to identify the potential security risks or weaknesses.

User Acceptance Testing (UAT):

- **Manual Testing:** Although it is not a particular device, manual testing of the system by the end-users or stakeholders can be a great way to perform user acceptance testing and collect the feedback of the system's usability, functionality, and overall satisfaction.
- **User Feedback Tools:** Applications such as Google Forms, SurveyMonkey, or UserVoice can be used to get the feedback from the users and stakeholders about their experience with the system.

4.2 Test Cases and Outcomes

Test Cases:

4.2.1 Unit Testing:

- **Face Detection Module:**
  - Check the precise detection of faces in good light.
  - Test the face detection in the low light conditions.
  - Find the confirmation of detection with different faces orientations (frontal, side, tilted).

    - Make sure that the detection is robust by using images that have multiple faces.
    - Confirm that detection accuracy is still high when the vehicle has occlusions.

- **Face Recognition Module:**
    - Validate the correct detection of faces of enrolled users.
    - The recognition of the tests with different facial expressionsis necessary.
    - The recognition accuracy is checked out by different people of similar appearance.
    - The task is to let the unrecognized faces be rejected.
    - The recognition speed and accuracy of the system can be checked with a big dataset of the members who are enrolled.

- **Attendance Tracking:**
    - Check if the attending is correctly recorded upon the successful attendance.
    - Testing the logging of the function with multiple recognition occurrences at the same time.
    - Ensure the validity of the timestamps in attendance records.
    - Make sure that the way of recognising the failures of the problem is correctly done (e. g. warning systems). g. , unrecognized faces).

4.2.2 Integration Testing:

- **Face Detection and Recognition Integration:**
    - Make sure to verify the smooth connection of face detection and recognition modules.
    - Guarantee the right passing of detected faces to the recognition module.
    - Test integration soundness taking into account the quick and accurate identification and recognition of the sequences.

- **Recognition and Attendance Tracking Integration:**

    - The attendance should be recorded based on the results of recognition to be accurate.
    - Check the consistency of validated users and logged attendance records.

4.2.3 End-to-End Testing:

- **Attendance Process:**
    - Exam the whole attendance procedure from its initiation to its logging.
    - Assume the user interactions involving the start of the attendance process, capturing images, and logging attendance.
    - Check for the correctness and the completeness of attendance records.

4.2.4 Regression Testing:

- **Functionality Regression:**
    - Test existing test cases after system updates in order to see if there are any new regressions.
    - Check if backward compatibility with the versions of the system that were used before is really possible.

4.2.5 Performance Testing:

- **System Response Time:**
    - The assignment is to measure the response time under different load levels.
    - Check the reliability of the system when the large number of faces is being processed at the same time.

4.2.6 Security Testing:

- **Data Security:**
    - Check if the data encryption is done for the sensitive data.
    - Check the access control ways to stop the unauthorized access.
    - Find out the level of resistance to spoofing attacks that use fake faces or photos.

4.2.7 User Acceptance Testing (UAT):

- **Usability Testing:**
  - Get feedback from the final users on system usability, interface design, and the level of the ease of use.
  - Approve the user satisfaction with the system's performance and functioning.

Outcomes:

- **Functional Validation:** The evidence that the system is able to correctly detect and recognize faces, attendance is logged correctly, and performs other important functions as required signals the system's efficiency.

- **Performance Assessment:** The system's performance metrics such as response time, throughput, and resource utilization are measured under various load levels and environmental conditions .

- **Security Evaluation:** Determination of possible security weaknesses and threats, along with the suggestions of the measures for the avoidance of these weaknesses and threats in order to boost the data security and protect against the threats such as unauthorized access and spoofing attacks.

- **Usability Feedback:** User feedback on the system's usability, interface design, and overall user experience, which in turn gives more information for the optimization and improvement of the system.

- **Bug Detection and Regression Prevention:** The detection and solution of software bugs, and the prevention of regressions through the rigorous regression testing and the validation of backward compatibility are among the tasks performed by the developers.

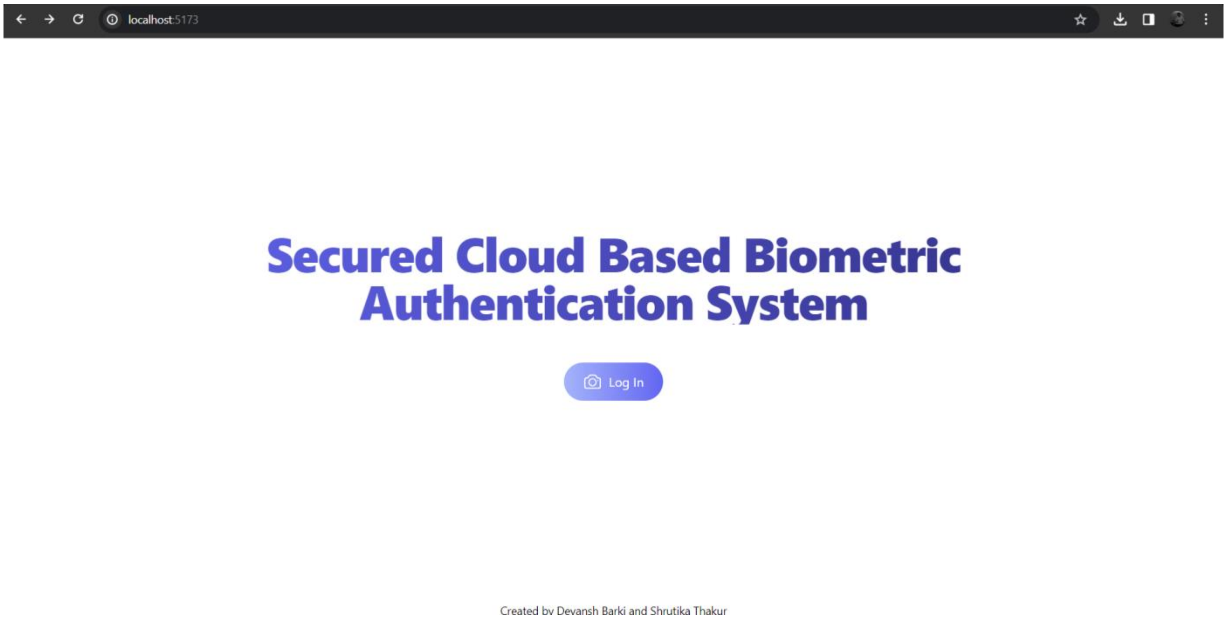
- **Compliance Verification:** The verification of conformity to regulatory requirements and industry standards on data privacy, security and accessibility is the yardstick of the author's task.

- **User Satisfaction:** Evaluation of the users satisfaction with the system's performance, functionality, and the ease of use, which will help in the future the development of the system and the feature enhancement based on the users needs and preferences.

- **Validation of Business Requirements:** The face-based attendance system is checked and matched with the predefined business requirements and objectives, and this process is done to make sure that it is in line with the organizational goals and expectations.

Chapter 5: Results and Evaluation

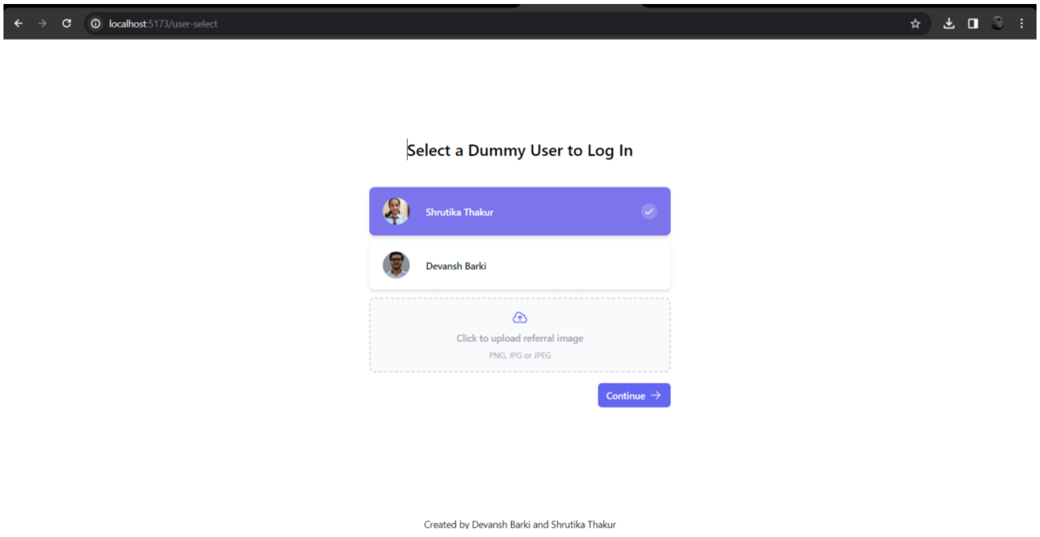
5.1 Results



Secured Cloud Based Biometric Authentication System

Created by Devansh Barki and Shrutika Thakur

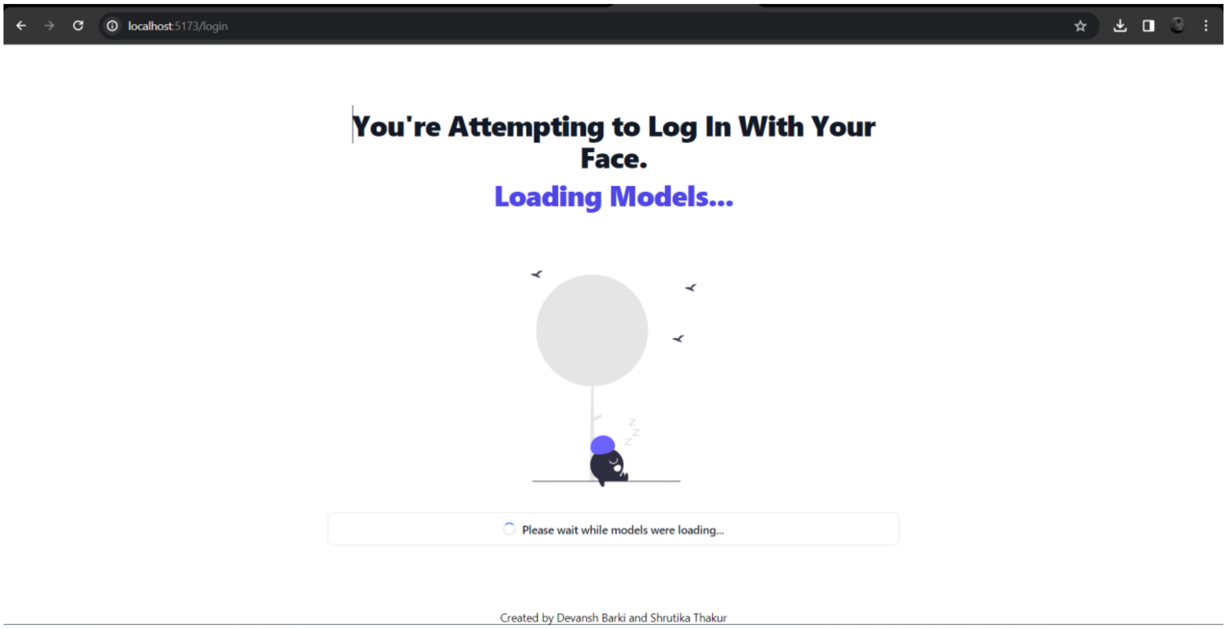
Figure:5.1 Home Page



Select a Dummy User to Log In

Created by Devansh Barki and Shrutika Thakur

Figure:5.2 Login Page



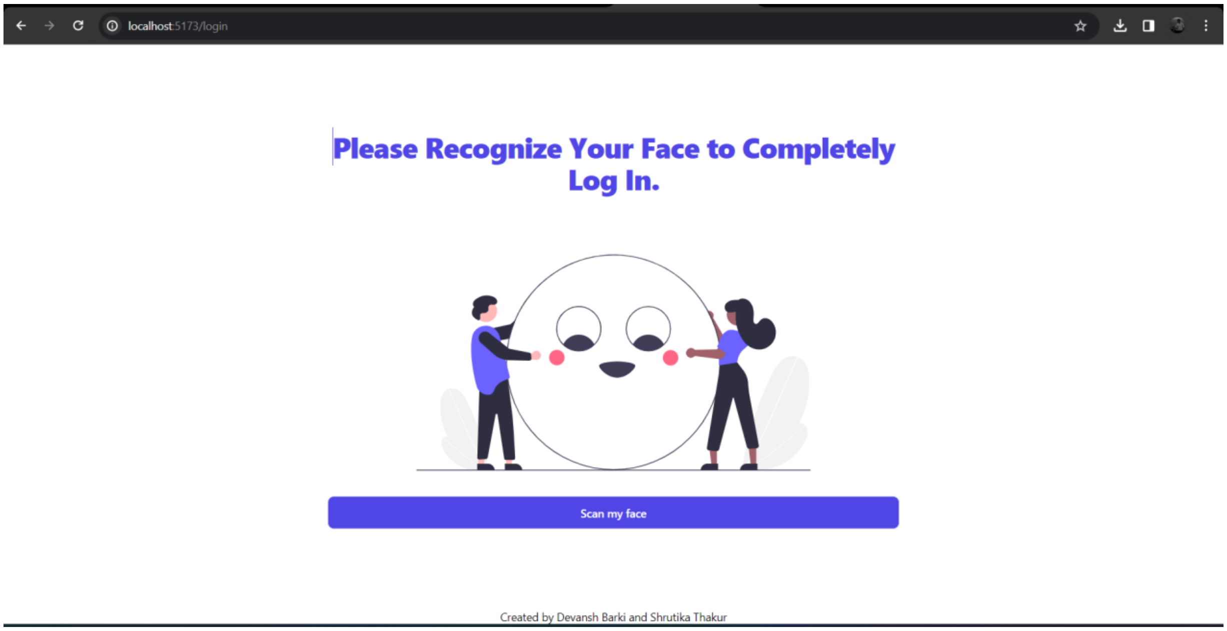
You're Attempting to Log In With Your Face.

Loading Models...

Please wait while models were loading...

Created by Devansh Barki and Shrutika Thakur

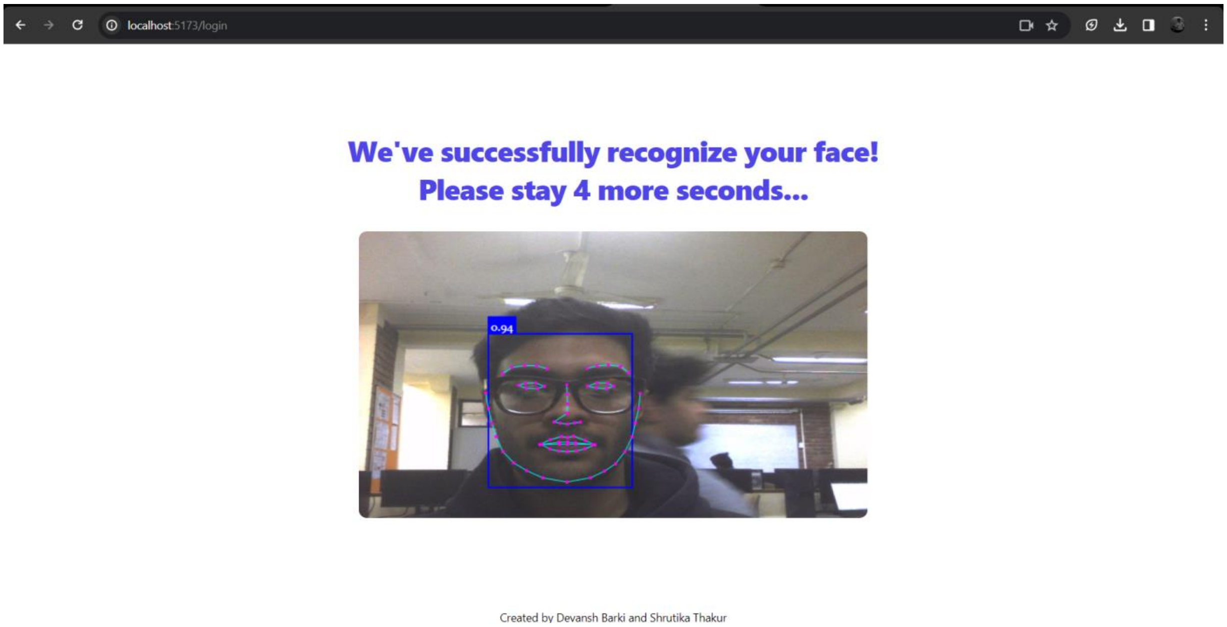
Figure: 5.3 waiting



Please Recognize Your Face to Completely Log In.

Created by Devansh Barki and Shrutika Thakur

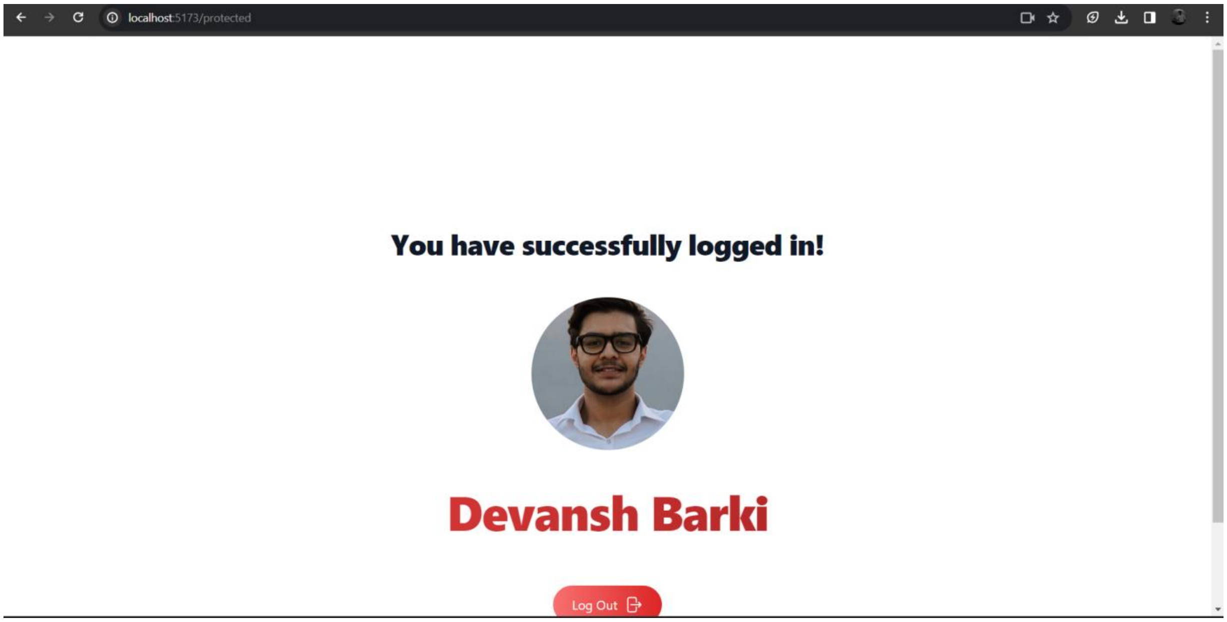
Figure :5.4 Processing to recognize the face



We've successfully recognize your face!
Please stay 4 more seconds...

Created by Devansh Barki and Shrutika Thakur

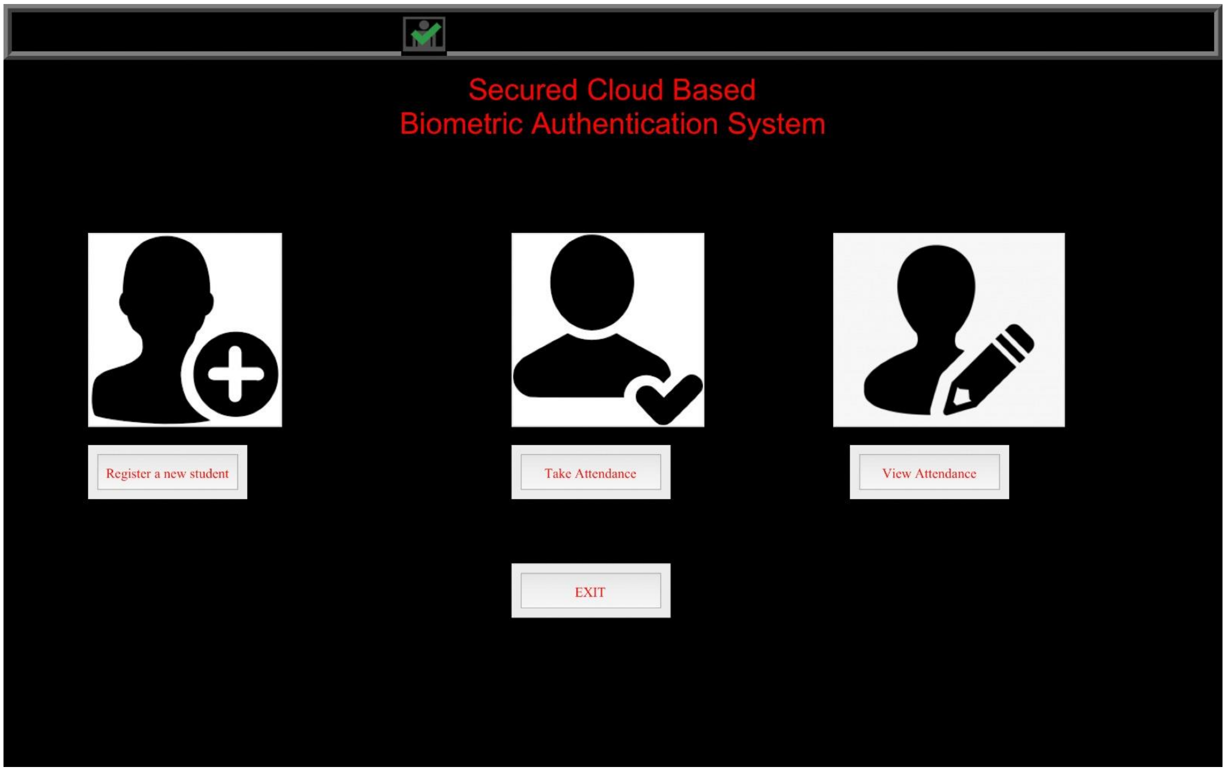
Figure:5.5   waiting to get logged in



You have successfully logged in!

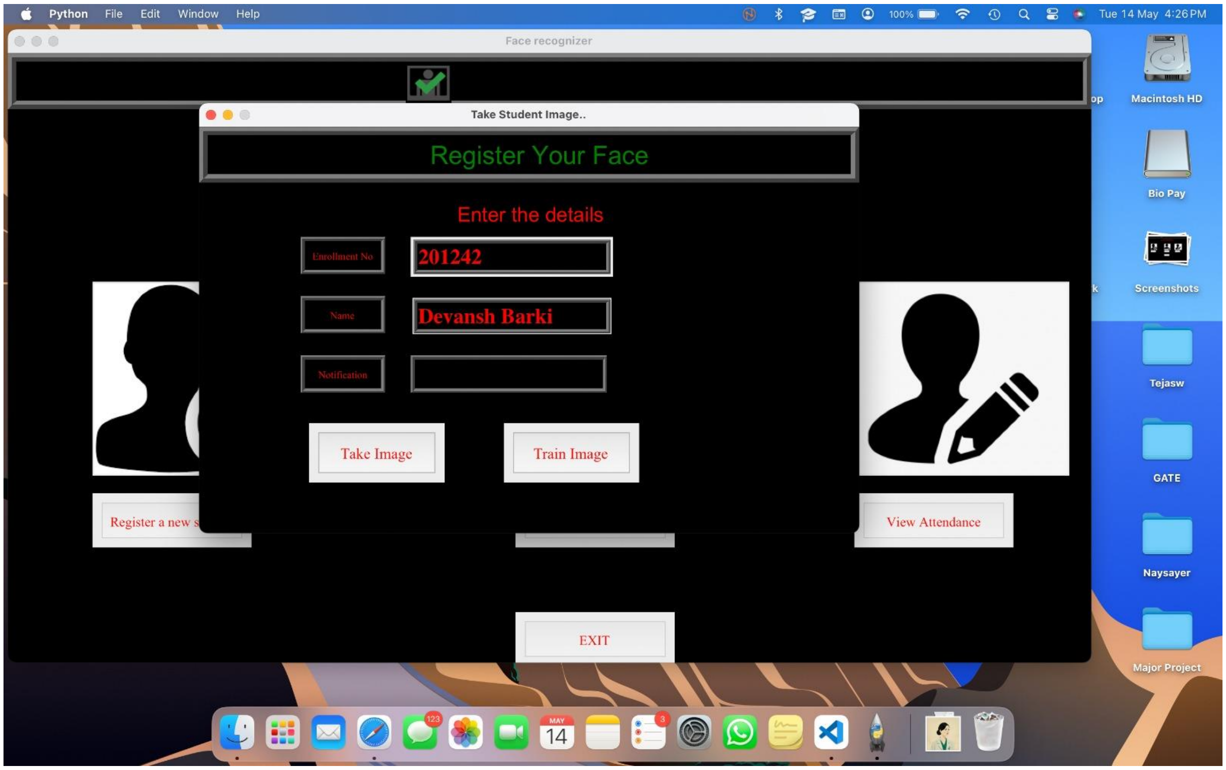
Devansh Barki

Figure:5.6 successfully logged in



Secured Cloud Based
Biometric Authentication System

Fig . 5.7 Home Page for the cloud based attendance system



Register Your Face

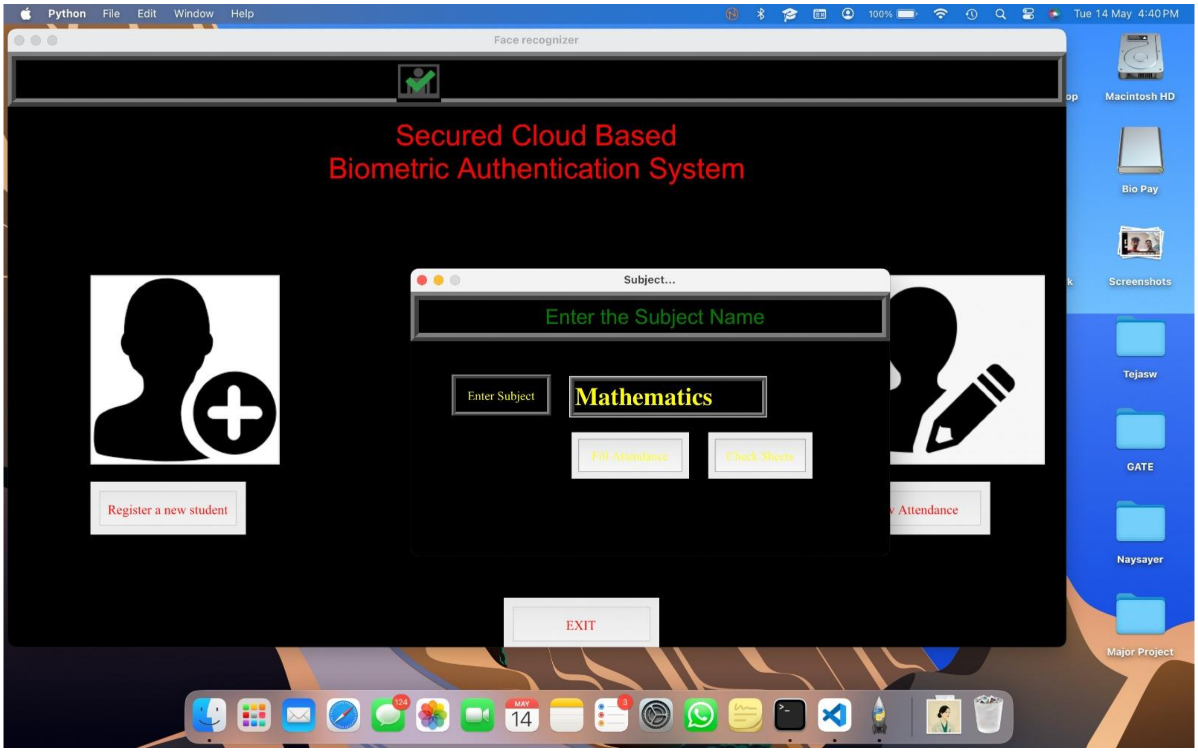
Enter the details

Enrollment No: 201242

Name: Devansh Barki

Notification:

Fig. 5.8 Registering The Face



Secured Cloud Based
Biometric Authentication System

Enter the Subject Name

Mathematics

Fig . 5.9 Choosing the subject name

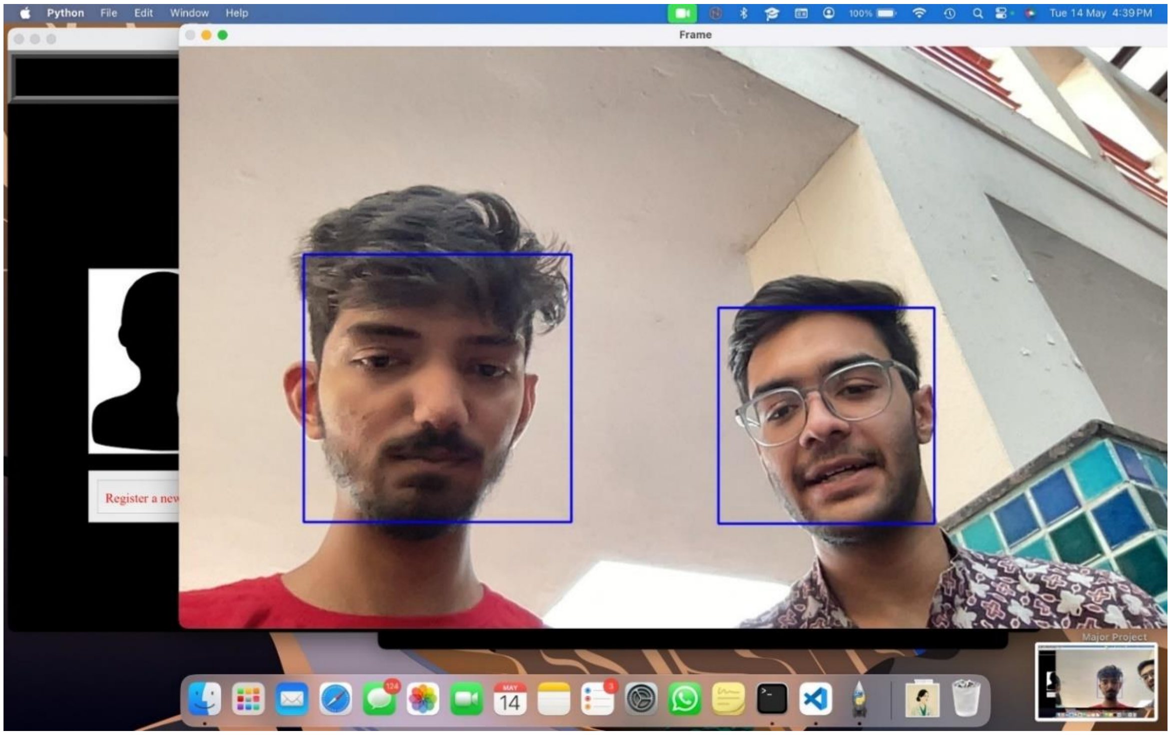


Fig 5.10 Training the images

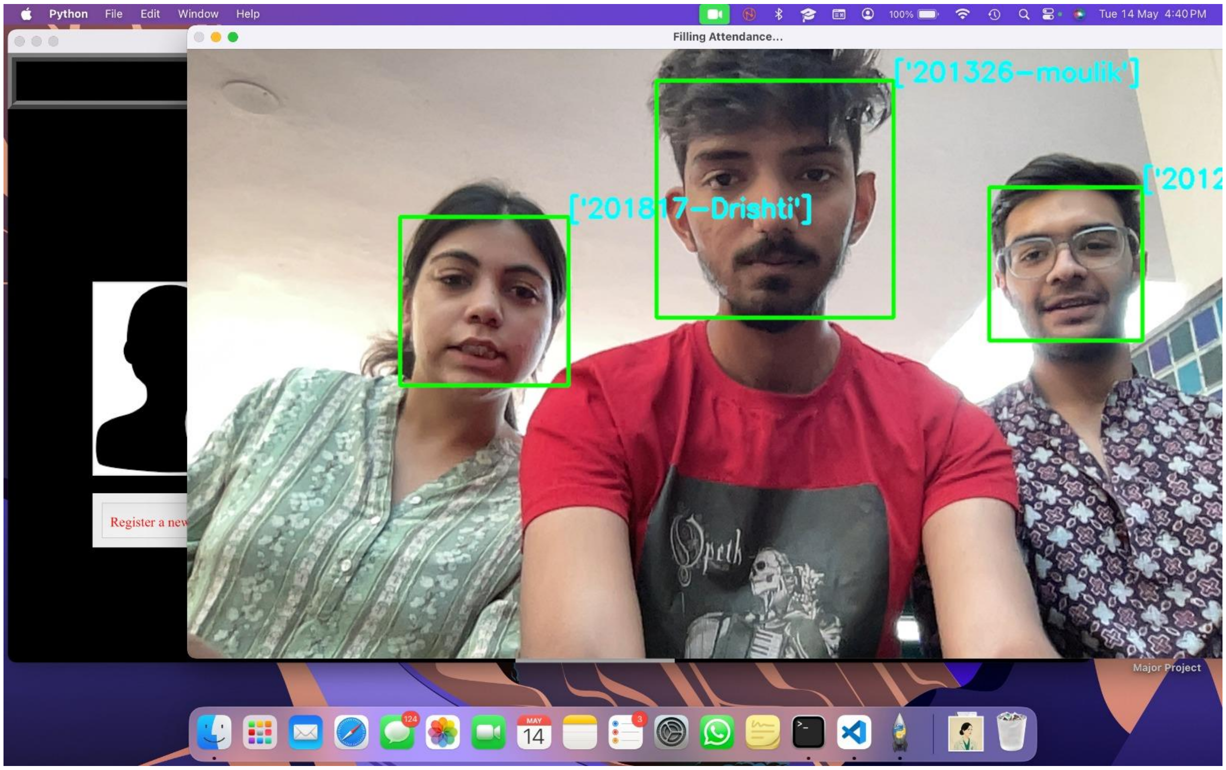
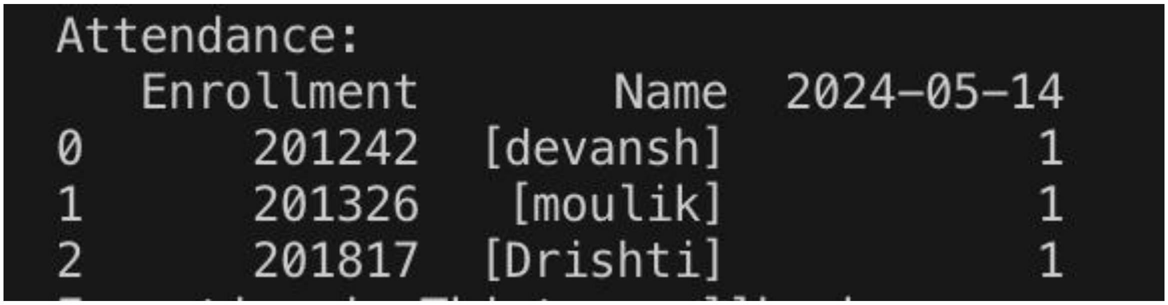


Fig .5.11 Taking Attendance



```
Attendance:
   Enrollment        Name  2024-05-14
0      201242   [devansh]           1
1      201326    [moulik]           1
2      201817   [Drishti]           1
```

Fig . 5.12 Attendance record

Chapter 6: Conclusions and Future Scope

5.1 Conclusion

In conclusion, the project on secure cloud-based biometric authentication stands as a crucial advancement in addressing contemporary challenges within identity verification systems. The fusion of biometric traits with cloud technology not only fortifies security but also provides a user-friendly and globally accessible solution. The successful achievement of project objectives, including the establishment of robust encryption mechanisms, accurate recognition algorithms, and a seamless authentication process, highlights its effectiveness.

The project's significance is underscored by its capacity to mitigate cyber security risks associated with traditional authentication methods, offering a more resilient defense against evolving threats. The user-centric approach ensures a streamlined and efficient authentication experience, eliminating the need for complex passwords and reducing the susceptibility to common security vulnerabilities.

Moreover, the exploration of privacy-preserving measures, such as encrypting biometric data before outsourcing it to the cloud, underscores a commitment to safeguarding user privacy. The proposed system's resilience to potential attacks, including those attempting to mimic detection requests and collude with the cloud, underscores its robustness in real-world scenarios.

The project's contribution extends beyond technological advancements, incorporating elements of cost-effectiveness by leveraging cloud infrastructure and scalability to adapt to varying user demands. Adhering to data protection regulations and fostering user trust aligns with ethical considerations and regulatory requirements, ensuring responsible handling of sensitive biometric information.

In essence, the secure cloud-based biometric authentication project signifies a significant step toward a more secure, efficient, and user-centric digital future. The successful implementation of the proposed system, as evidenced by improved performance metrics and comprehensive security measures, positions it as a viable and impactful solution in the realm of identity verification. As technological advancements endure, this project establishes the groundwork for upcoming innovations at the nexus of biometrics and cloud computing, thereby augmenting digital security and improving user experiences continuously.

5.2 Future Scope

Enhanced Accuracy and Robustness: The fact that ongoing research and development are necessary for enhancing the precision and stability of face detection and recognition algorithms cannot be overstated. These activities are the pursuits of the discovery of the cutting-edge preprocessing techniques and the feature extraction methods that are used to overcome the problems that are caused by the changing lighting, facial expressions, and occlusions. The combination of ensemble methods and fusion techniques can be a way of the increase of recognition accuracy by exploiting the strength of several algorithms. Moreover, the continuous improvement of algorithms and system architecture is needed if we want to obtain real-time performance and responsiveness, even on the hardware with the limited resources.

Real-Time Performance Optimization: Real-time performance in face-based attendance systems can be achieved by optimizing the algorithm implementations, parallel processing techniques and the hardware utilization. These improvements may be realized by the use of the hardware accelerators like GPUs and TPUs, efficient data structures, and the caching mechanism to cut down the latency and at the same time, to achieve the maximum throughput.

Through the optimization of system performance, attendance tracking can be done smoothly in real-time and, thus, the users will be provided with instant feedback and the whole system efficiency and usability will be enhanced.

Multi-Modal Biometric Fusion: The combination of different biometric modalities, like fingerprint recognition, iris recognition, and voice recognition, gives a new promising way for the improvement of the security and reliability of the attendance systems. Through the fusion of the data from the different biometric modalities by the fusion techniques the system can reach the maximum of accuracy and robustness. The adaptive fusion algorithms can change the fusion strategies according to the quality and reliability of the input modalities and hence, can be used in various situations to ensure the best possible performance.

Adaptive Learning and Personalization: Adaptive learning algorithms are the ones that are very important in the case of the recognition accuracy which keeps on improving with time. Through the use of user feedback and system performance metrics, these algorithms can continuously modify the recognition models to fit to the changes of conditions and user preferences. Personalization features, in turn, improve user experience by customizing the system's behavior and preferences to the specific needs and preferences of individual users, thus, the system becomes more usable and the users are more satisfied.

Scalability and Cloud Integration: Creating face-oriented attendance systems that are scalable and cloud-ready will allow them to meet the needs of growing user bases and increasing data volumes. Cloud integration allows the uninterrupted deployment across the different environments, which ensures the scalability, flexibility, and the on-demand resource provisioning. With containerization and microservices architectures, the deployment and management of systems in cloud environments becomes a lot easier, thus, they provide agility and scalability when the system requirements change.

Mobile and IoT Integration: Apps and IoT devices enable the attendance tracking to be improved and the user engagement to be increased. Mobile apps are used to record the attendance data of users with the help of their smartphones or tablets, while IoT devices such as smart cameras and sensors assist in the automated attendance monitoring and real-time data capture. Through the link of edge computing methods, attendance tracking can be done on-device, thus cutting down the dependence on centralized servers and at the same time, the speed of response is increased in remote or disconnected areas.

Advanced Security Features: Since face-based attendance systems deal with sensitive biometric data, it is very important to have advanced security features in them to prevent the unauthorized access and security breaches. These features might be for instance the biometric encryption, multi-factor authentication mechanisms, and anti-spoofing techniques like the liveness detection. Through the security of attendance data, organizations can safeguard the integrity and the confidentiality of the attendance data which will result in user trust and the compliance of the regulatory requirements.

Analytics and Insights: The statistics and reports about attendance provide critical information about the attendance data which allows organizations to discover trends, patterns, and anomalies. Predictive analytics models help in the forecasting of the attendance trends and the allocation of resources is also optimized while the interactive dashboards and the visualization tools are used in the decision-making process and the strategic planning. Through the use of analytics, organizations can get out of the data what can be the actions derived from the attendance and as a result they will be able to constantly improve and to make the informed decisions.

References:

[1].El-El-Sofany, Hosam. "A Proposed Biometric Authentication Model to Improve Cloud Systems Security." *Computer Systems Science & Engineering* 43.2 (2022).

[2]. Shakil, Kashish Ara, et al. "BAMCloud: a cloud based Mobile biometric authentication framework." *Multimedia Tools and Applications* (2022): 1-30.

[3]. Prabhu, D., S. Vijay Bhanu, and S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment." *Measurement: Sensors* 24 (2022): 100511.

[4]. Venkatachalam, K., et al. "Secure biometric authentication with deduplication on distributed cloud storage." *PeerJ Computer Science* 7 (2021): e569

[5]. Lokhande, Trupti, Shrikant Sonekar, and Aachal Wani. "Development of an Algorithmic Approach for Hiding Sensitive Data and Recovery of Data based on Fingerprint Identification for Secure Cloud Storage." *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2021.

[6]. Al-Assam, Hisham, Waleed Hassan, and Sherali Zeadally. "Automated biometric authentication with cloud computing." *Biometric-based physical and cybersecurity systems* (2019): 455-475.

[7]. Jaichandran, R. "Biometric based user authentication and privacy preserving in cloud environment." *Turkish Journal of Computer and Mathematics Education (TURNCOAT)* 12.2 (2021): 347-350.

[8]. Yadav, Bonthala Prabhanjan, et al. "A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing." *IOP Conference Series: Materials Science and Engineering*. Vol. 981. No. 2. IOP Publishing, 2020.

[9]. Shakil, Kashish A., et al. "BAMHealthCloud: A biometric authentication and data management system for healthcare data in the cloud." *Journal of King Saud University-Computer and Information Sciences* 32.1 (2020): 57-64.

[10]. Liu, Chun, et al. "An efficient biometric identification in cloud computing with enhanced privacy security." *IEEE Access* 7 (2019): 105363-105375.

[11]. Sumit Jaiswal ,Subhash Chandra Patel, Santosh Kumar, R. S. Singh, S. K. Singh “Biometric Authentication for Cloud Service Provider in Multiple Cloud Storage System” 10.4018/978-1-5225-7501-6.ch071 2019.

[12]. Zhu, Hua-Hong, et al. "Voiceprint-biometric template design and authentication based on cloud computing security." *2011 International Conference on Cloud and Service Computing*. IEEE, 2011.

[13]. Panchal, Gaurang, et al. "Designing Secure and Efficient Biometric-Based Access Mechanism for Cloud Services." *IEEE Transactions on Cloud Computing* 10.2 (2020): 749-761.

[14]. Nakouri, Ihsen, Mohamed Hamdi, and Tai-Hoon Kim. "A new biometric-based security framework for cloud storage." *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017.

[15].https://www.researchgate.net/figure/Biometric-Techniques-to-Secure-Cloud-Computing_fig3_317253286

[16]. https://legacy.reactjs.org/docs/getting-started.html

[17]. https://justadudewhohacks.github.io/face-api.js/docs/index.html

[18].https://www.igi-global.com/chapter/biometric-authentication-for-the-cloud-computing/217892

[19]. https://aws.amazon.com/rekognition/identity-verification/

[20]. https://docs.docker.com/engine/security/

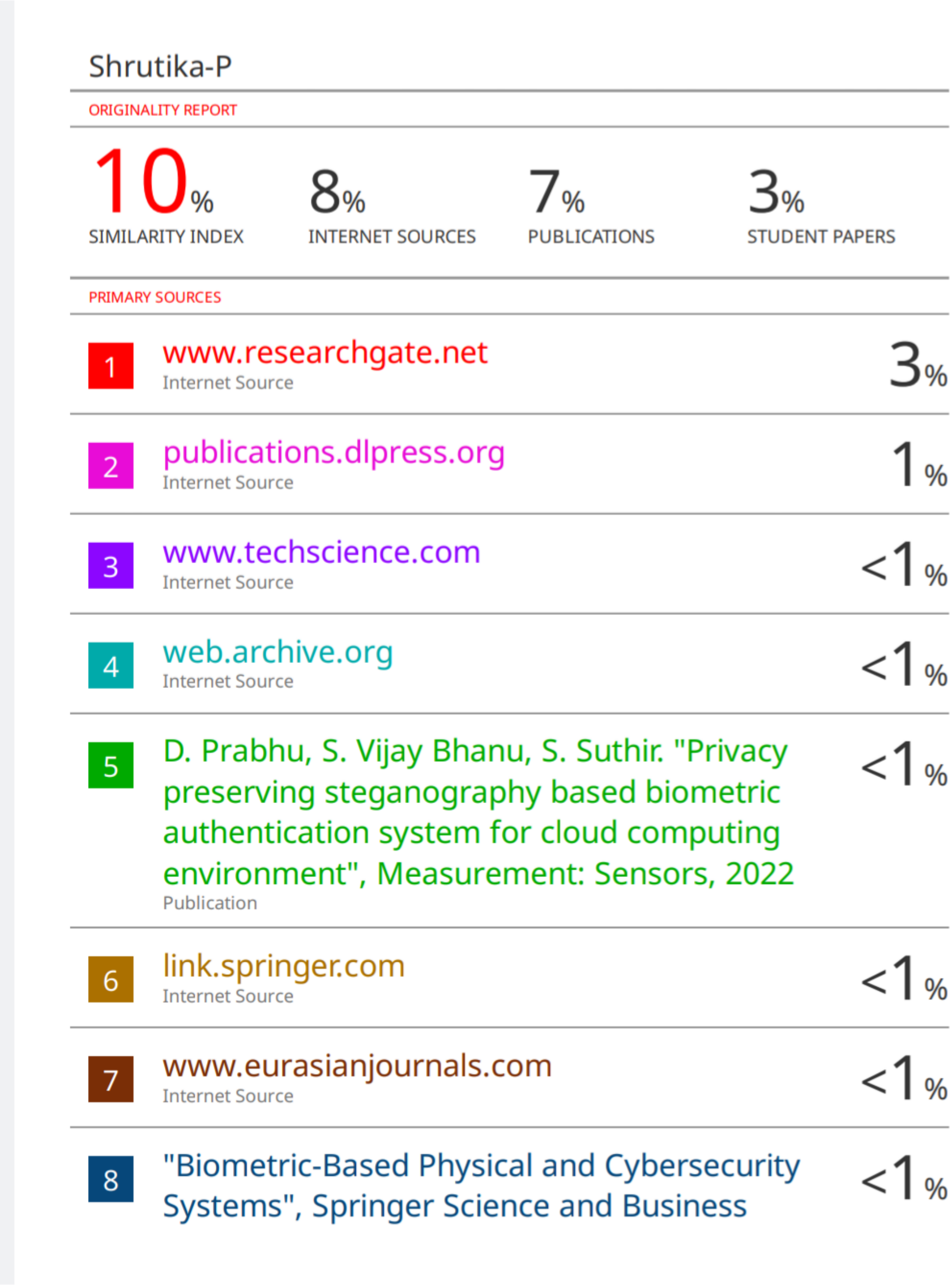
[21]. Ziyad, Shabana, and A. Kannammal. "A multifactor biometric authentication for the cloud." *Computational Intelligence, Cyber Security and Computational Models: Proceedings of ICC3, 2013*. Springer India, 2014.

[23]. Dharavath, Krishna, Fazal A. Talukdar, and Rabul H. Laskar. "Study on biometric authentication systems, challenges and future trends: A review." *2013 IEEE international conference on computational intelligence and computing research*. IEEE, 2013.

[24]. Snelick, Robert, et al. "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems." *IEEE transactions on pattern analysis and machine intelligence* 27.3 (2005): 450-455.

[25]. Albahdal, Abdullah A., and Terrance E. Boult. "Problems and promises of using the cloud and biometrics." *2014 11th International Conference on Information Technology: New Generations*. IEEE, 2014.

Appendix:



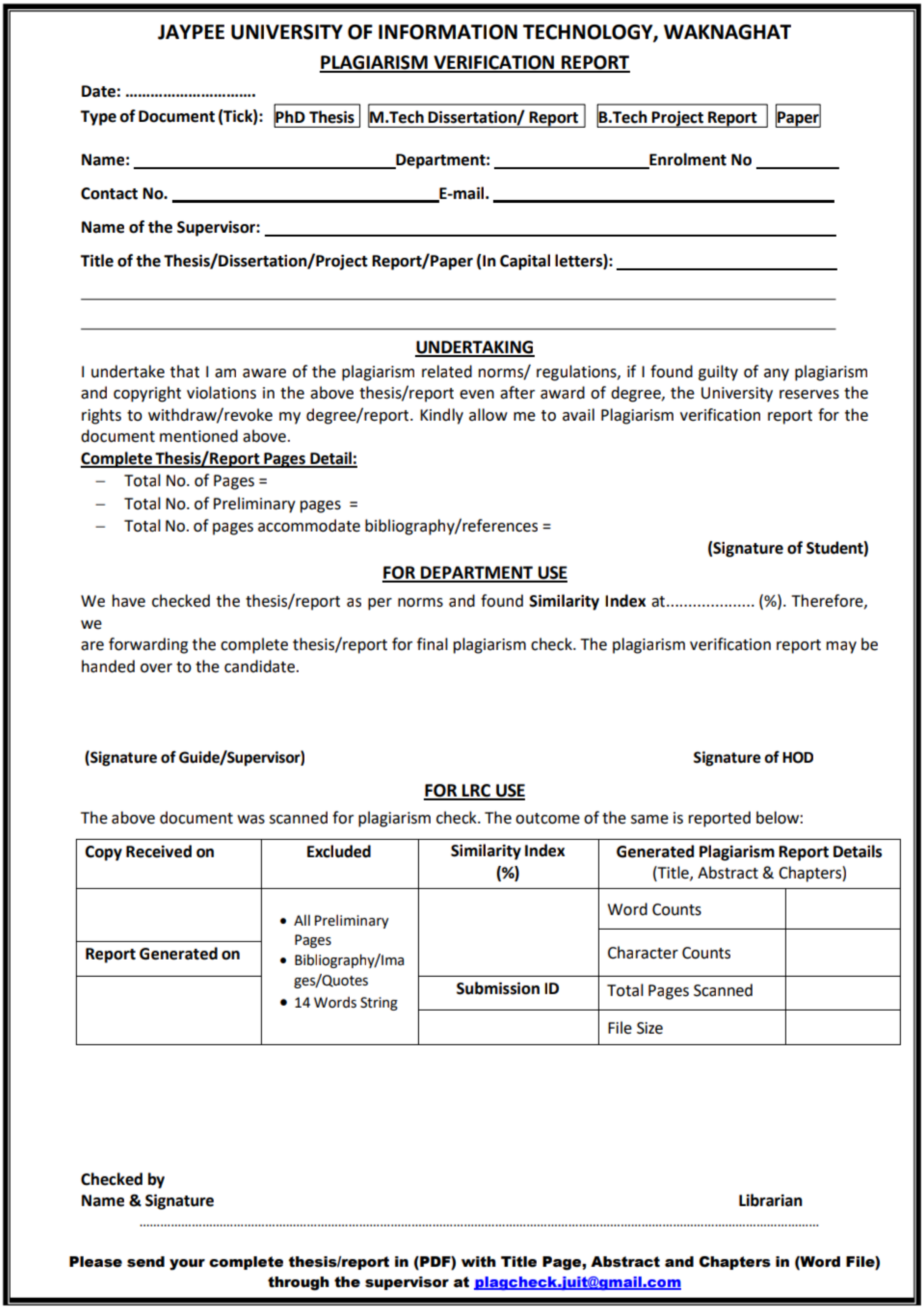
Shrutika-P

ORIGINALITY REPORT

10%	8%	7%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	3%
2	publications.dlpress.org Internet Source	1%
3	www.techscience.com Internet Source	<1%
4	web.archive.org Internet Source	<1%
5	D. Prabhu, S. Vijay Bhanu, S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment", Measurement: Sensors, 2022 Publication	<1%
6	link.springer.com Internet Source	<1%
7	www.eurasianjournals.com Internet Source	<1%
8	"Biometric-Based Physical and Cybersecurity Systems", Springer Science and Business	<1%



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: ....

Type of Document (Tick): **PhD Thesis** **M.Tech Dissertation/ Report** **B.Tech Project Report** **Paper**

Name: ______________________________ **Department:** __________________ **Enrolment No** __________

Contact No. ______________________________ **E-mail.** ____

Name of the Supervisor: ____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): __________________________

____

____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

– Total No. of Pages =
– Total No. of Preliminary pages =
– Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at.................. (%). Therefore, we
are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	**Excluded**	**Similarity Index (%)**	**Generated Plagiarism Report Details** (Title, Abstract & Chapters)	
	• All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature **Librarian**

....

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com