Cloud Based Attendance System

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

Bachelor of Technology

in

Computer Science & Engineering / Information Technology

Submitted by

Manoj Mehta (201345)

Under the guidance & supervision of

Ms, Seema Verma

Department of Computer Science & Engineering and Information Technology

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

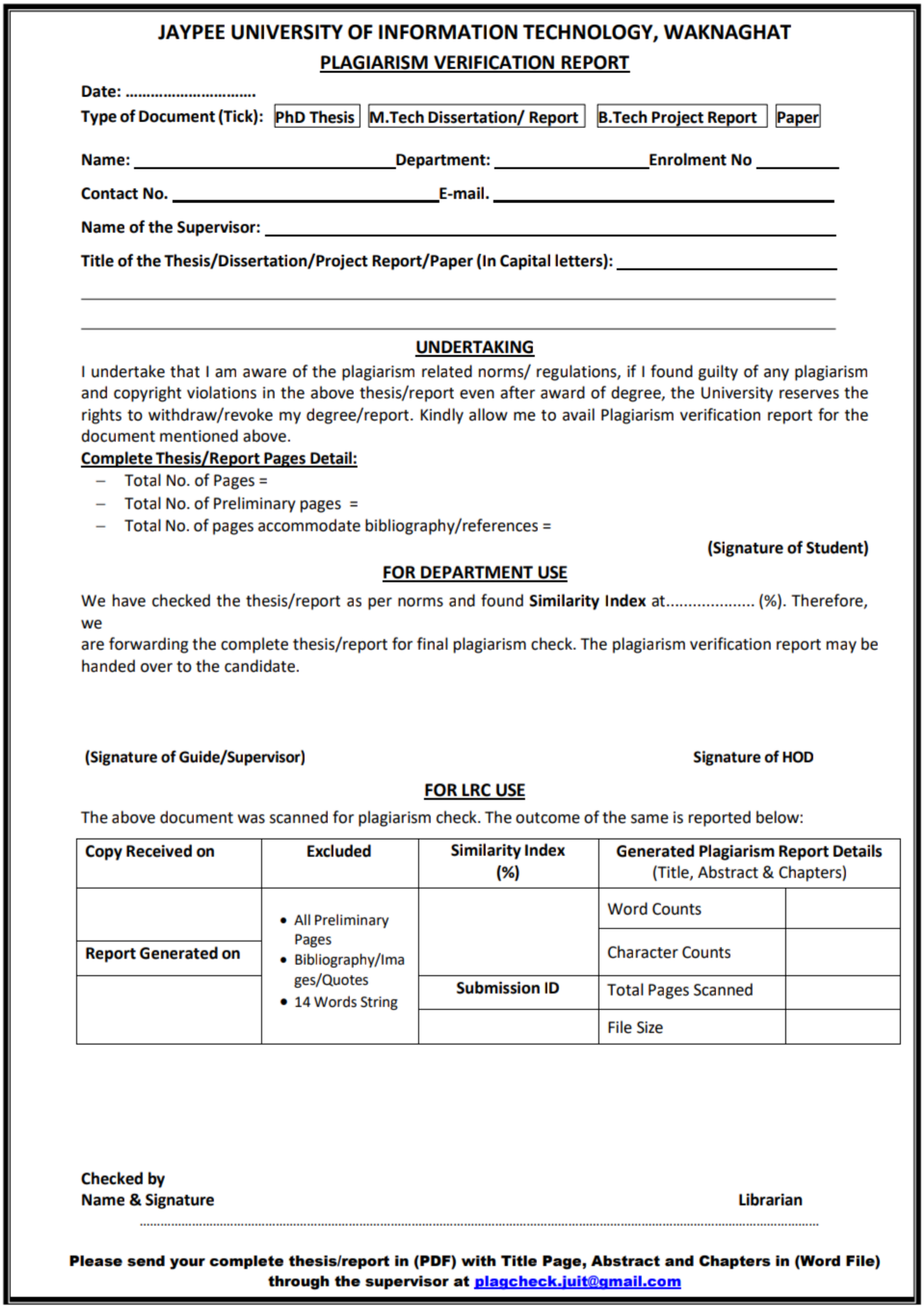
Certificate

This is to certify that the work which is being presented in the project report titled “ **Cloud Based Attendance System**” 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 “ **Manoj Mehta(201345)**” during the period from February 2024 to July 2024 under the supervision of **Ms. Seema Verma, Department of Computer Science and Engineering, Jaypee University of Information Technology,Waknaghat.**

Manoj Mehta(201345)

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

Ms, Seema Verma
Assistant Professor
Computer Science &Engineering and Information Technology
Jaypee University of Information Technology, Waknaghat,



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

Candidate's Declaration

I hereby declare that the work presented in this report entitled **'Cloud Based Attendance System'** 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 my own work carried out over a period from February 2024 to July 2024 under the supervision of **Ms. Seema Verma** (Assistant 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.

Manoj Mehta(201345)

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

Ms, Seema Verma
Assistant Professor
Computer Science And Engineering
10/07/2024

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to Ms, Seema Verma for helping me throughout the project and without whom this project would have been a very difficult task. I am highly indebted to ma’am for her guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in doing the project. She consistently motivated and guided me towards the completion of the project. I would like to express my gratitude towards my parents & members of JUIT for their kind cooperation and encouragement which helped me in doing this project. My thanks and appreciations also go to my colleagues who have helped me out with their abilities in developing the project.

Manoj Mehta(201345)

Table of Content

List of Tables

List of Figures

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 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 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 multi-device 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.

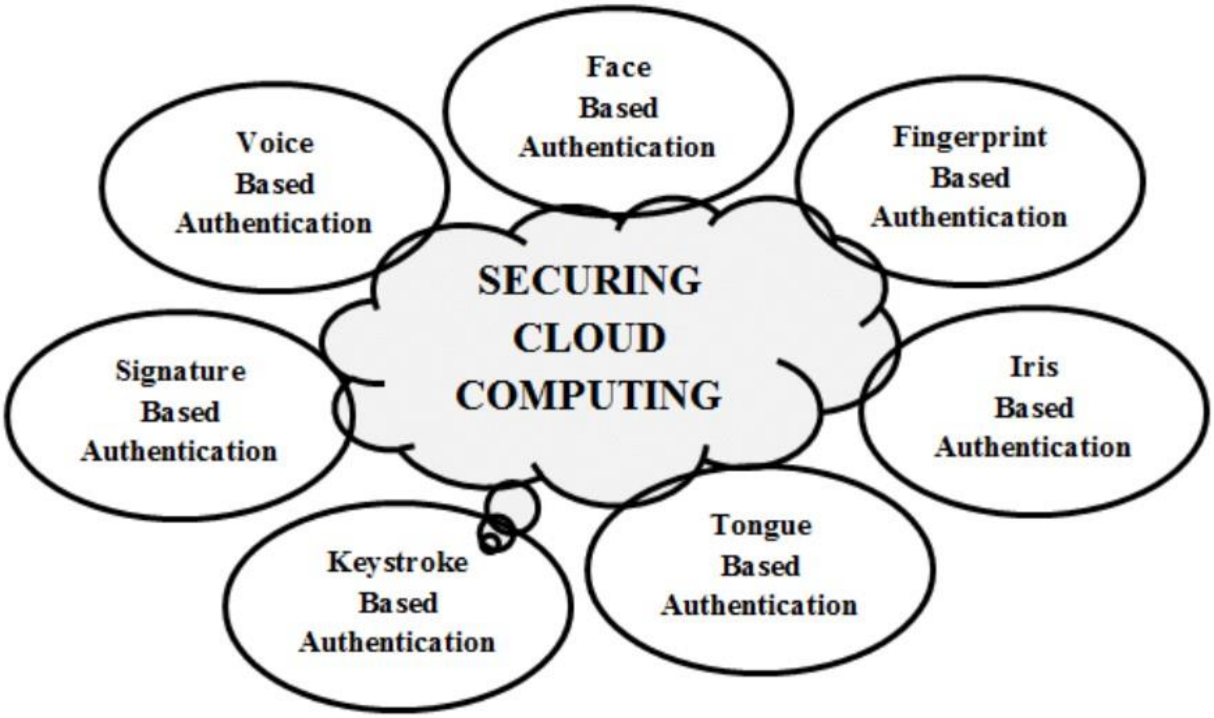

Face Based Authentication
Voice Based Authentication
Fingerprint Based Authentication
SECURING CLOUD COMPUTING
Signature Based Authentication
Iris Based Authentication
Keystroke Based Authentication
Tongue Based Authentication

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.

- **Enhanced Security:** 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 "Cloud Based Attendance System " 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 : 2.2.12.1 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 discrete wavelet transform (DWT) technique And continuous pigeon inspired optimizer (CPIO) algorithm,Q-learning technique	The proposed privacy preserving steganography based biometric authentication system (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 privacy preserving steganography based biometric authentication system (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:

- **User Enrollment:**The user's enrollment should capture, store and encode their facial images for identification purposes.The enrolment ought to be guided by a user interface.
- **Facial Recognition Authentication:**Users in the system should be authenticated on comparison of captured facial features with enrolled templates.Authentication should include real time face recognition.
- **User Management:** Administrators must be able to add new users as well as decommission old ones in this category of features.Defining user roles as well as corresponding permissions for administrative control.
- **User Feedback:** Offer straightforward feedback in the process of enrollment and authentication.Users are informed about completed or failed authentications.

Non-Functional Requirements:

- **Performance:** Users' experiences should be seamless since real-time facial recognition is expected.Enrollment and authentication latency in the system should be minimal.

- **Accuracy:** Therefore, a high accuracy rate for the face recognition algorithm should be maintained.Overtime, the accuracy can be improved through regular testing and tuning.

- **Security:**The facial features and templates should be kept safely guarded.Use encryption of data in transit and in place.To protect against some common security threats like spoofing.
- **Scalability:** The system should have the capacity for easy scaling for more users.The performance should not fall off with the increase of users.

- **Usability:** Both enrollment and authentication processes should require an intuitive user interface.Focus on usability issues, as some user populations have different needs.

- **Compatibility**: Compatibility across several gadgets and internet browsers.Therefore, they should implement responsive design for various screen sizes.

- **Error Handling:** Ensure that you put in place stringent error handling mechanisms for situations such as low light, failed face recognition processes etc.For users and the administrator, provide useful and well-defined error messages.

Analysis:

Architecture:

- **React Components:** Create React Enrollment, Authentication, User Management, and Feedback Components. Put the state management in place to deal with the various phases of facial detection.

- **Integration with face-api.js:** Facial recognition functionalities can be integrated with face-api.js library. Set up the library for instantaneous processing and facial features extraction.

- **Backend Integration:** Create user management and store the facial template APIs or backend services if needed.

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.

3.2 Project Design and Architecture Project

Design:

Algorithm:

- Start
- User Initiates Authentication
- Capture Biometric Data
- 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

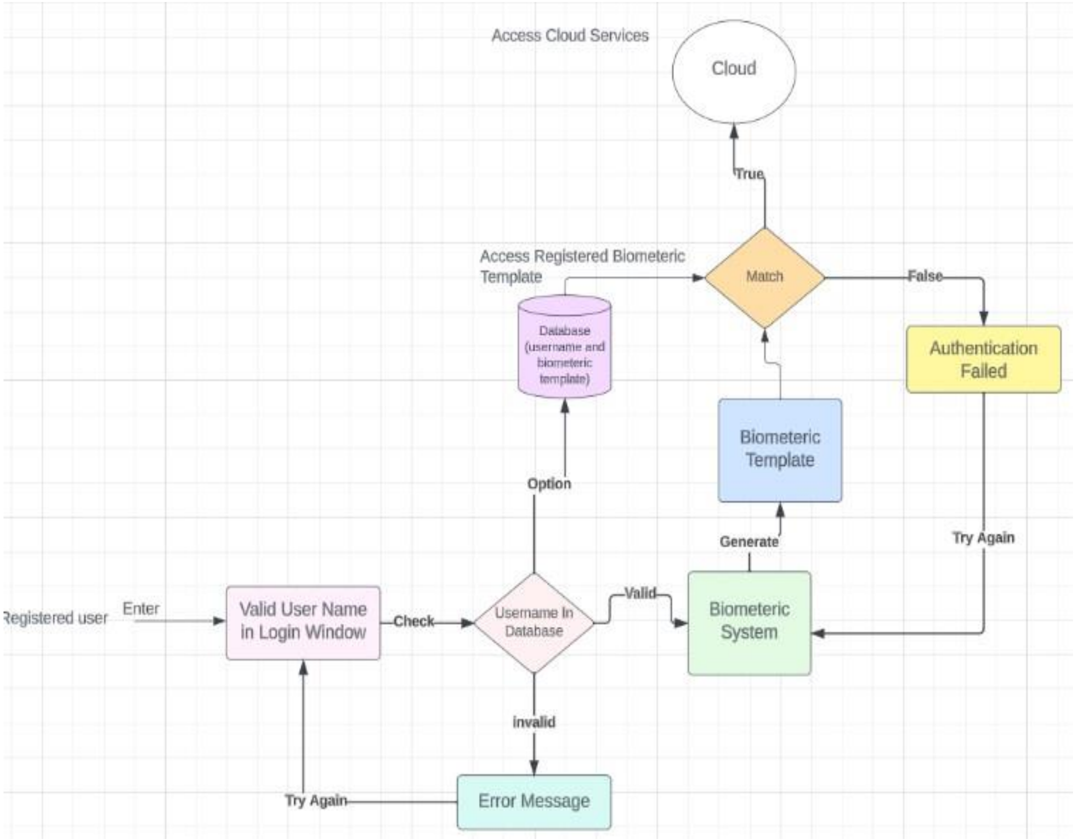


Figure 3.1: Project Design

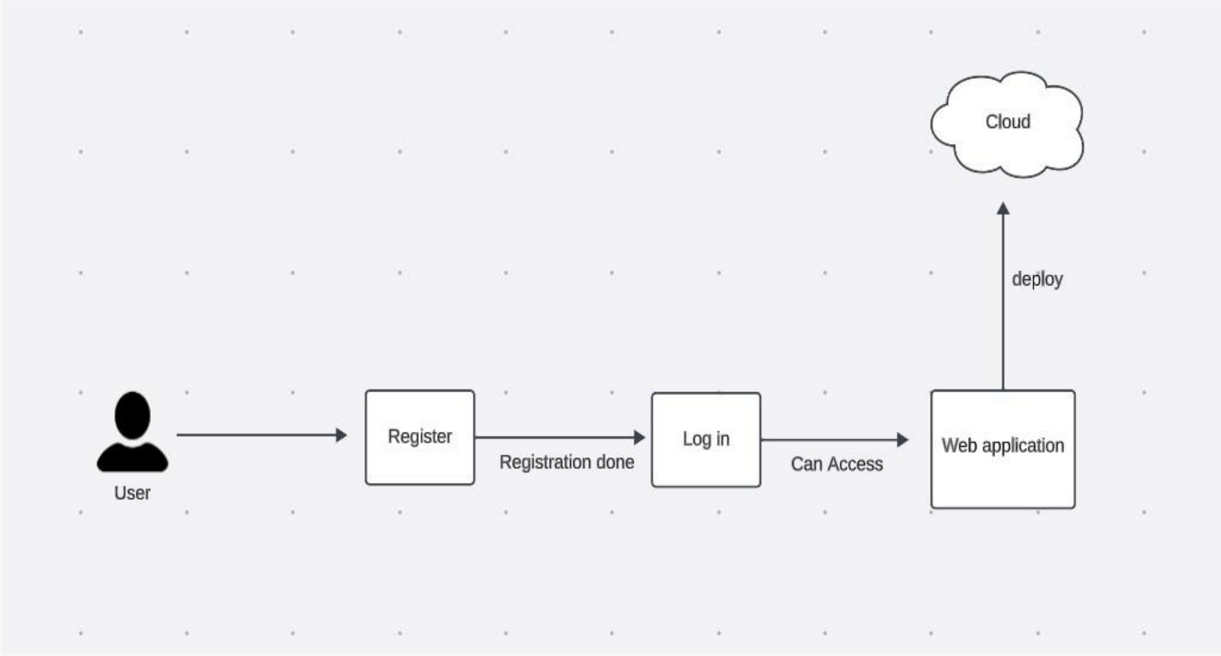


Figure 3.2: Project Workflow

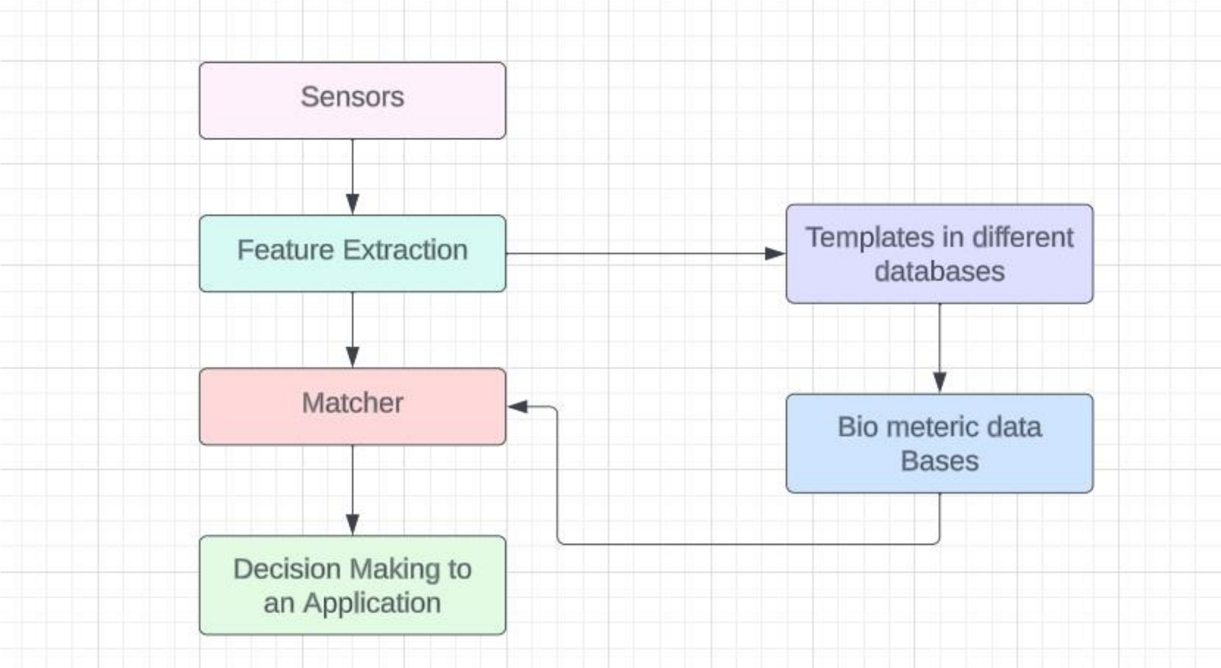

Sensors
Feature Extraction
Templates in different databases
Matcher
Bio meteric data Bases
Decision Making to an Application

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

3.3 Data Preparation

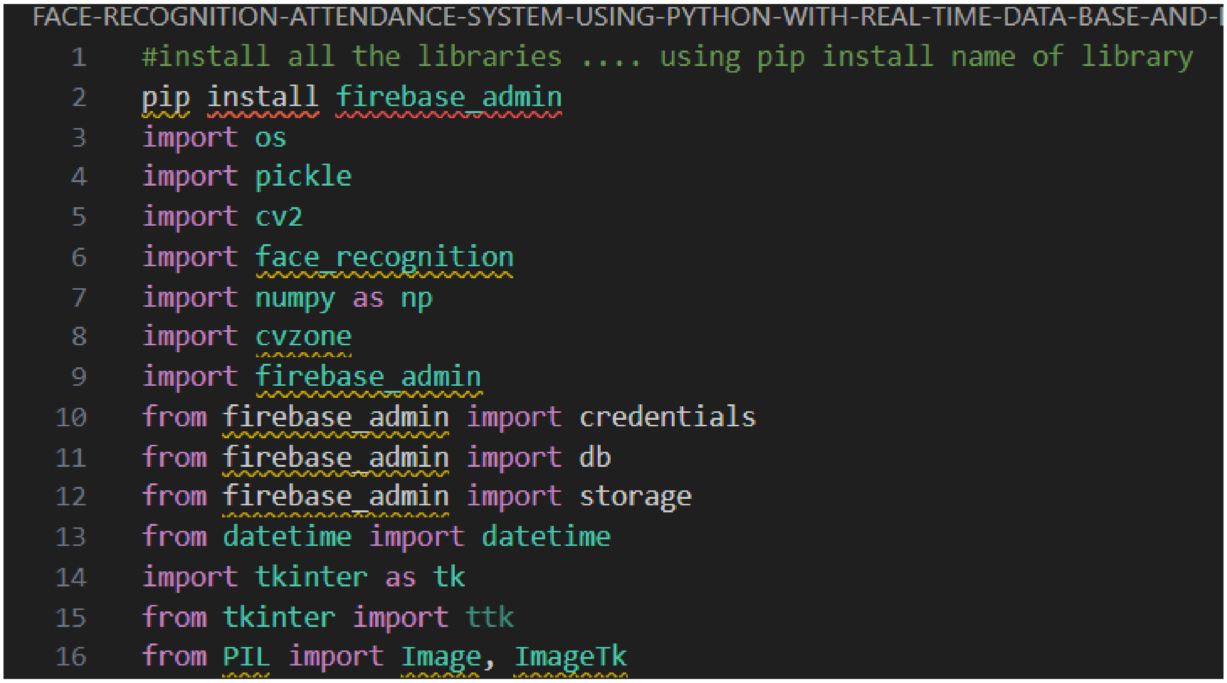
We have collected the data in the form of images by the help of a webcam. And that Data is being delivered for the authentication and privacy purpose of the web app. And the images will be fed to the system And then further registration will be performed and then we can login to our web application.

1.Data will be taken in form of images by using webcam

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 :

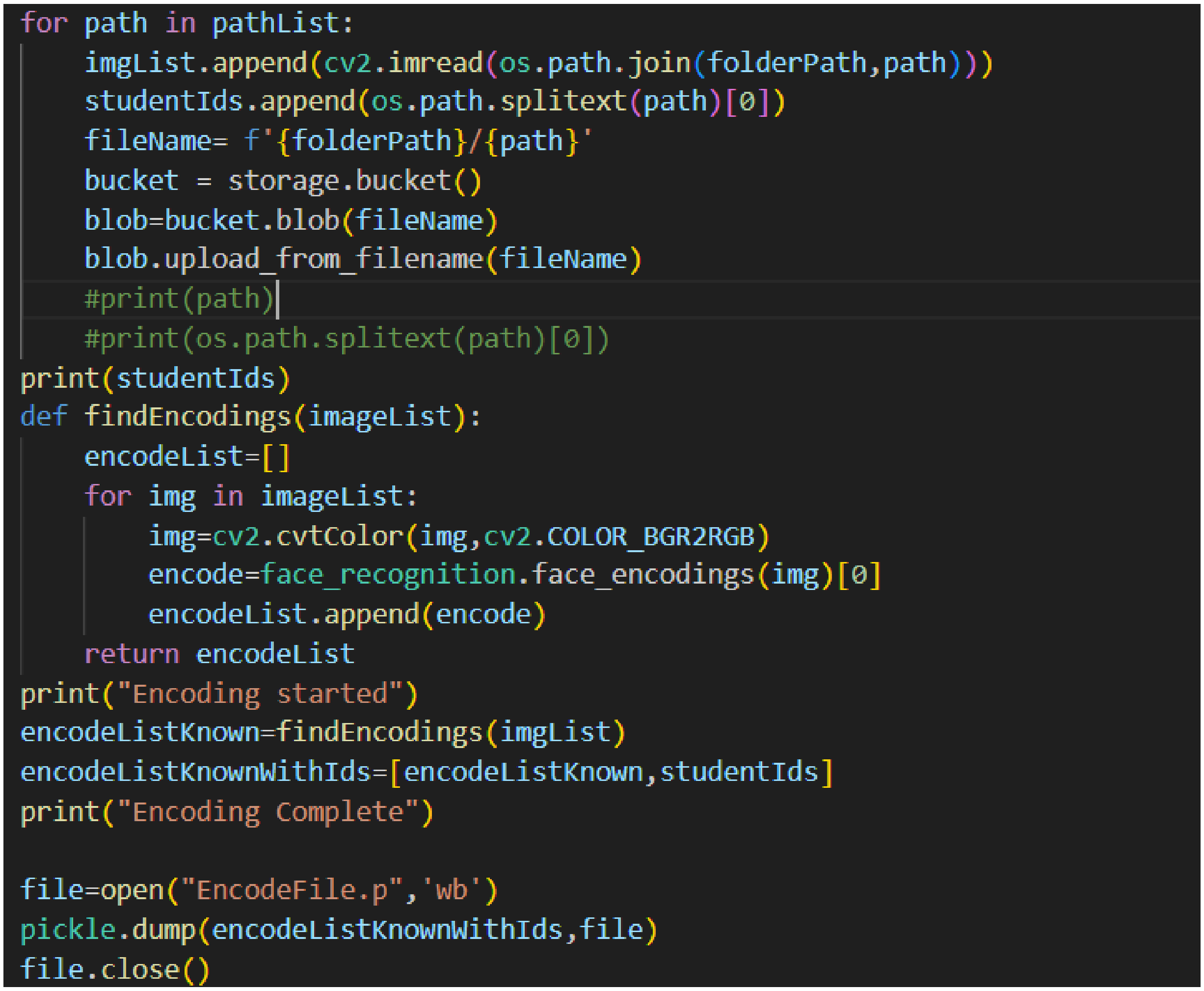
The goal of using React and face-api.js to implement a facial recognition-based authentication project is to seamlessly integrate state-of-the-art facial recognition capabilities into a safe and user-friendly interface. With the help of React, the project creates an easy-to-use interface and incorporates 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.



FACE-RECOGNITION-ATTENDANCE-SYSTEM-USING-PYTHON-WITH-REAL-TIME-DATA-BASE-AND-

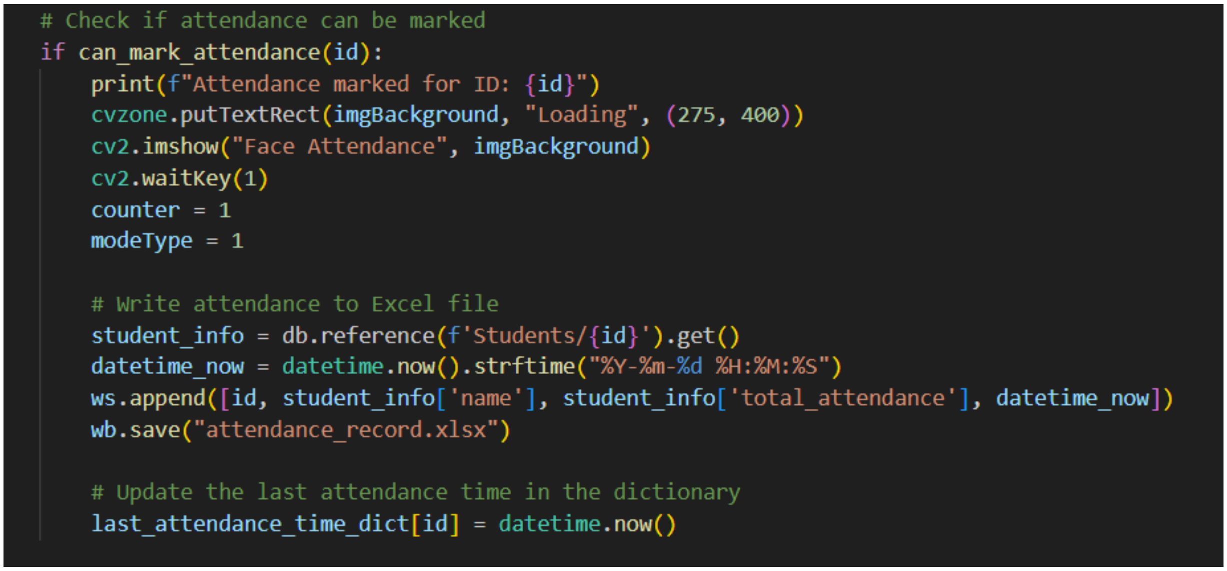
```
#install all the libraries .... using pip install name of library
pip install firebase_admin
import os
import pickle
import cv2
import face_recognition
import numpy as np
import cvzone
import firebase_admin
from firebase_admin import credentials
from firebase_admin import db
from firebase_admin import storage
from datetime import datetime
import tkinter as tk
from tkinter import ttk
from PIL import Image, ImageTk
```

Figure:3.4



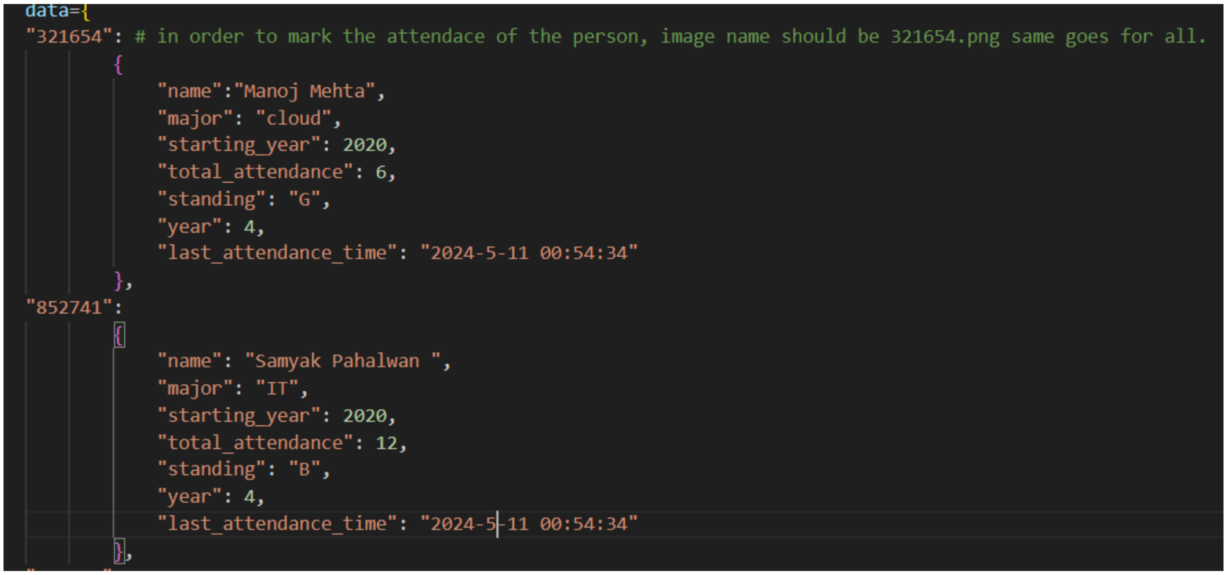
```python
for path in pathList:
    imgList.append(cv2.imread(os.path.join(folderPath,path)))
    studentIds.append(os.path.splitext(path)[0])
    fileName= f'{folderPath}/{path}'
    bucket = storage.bucket()
    blob=bucket.blob(fileName)
    blob.upload_from_filename(fileName)
    #print(path)
    #print(os.path.splitext(path)[0])
print(studentIds)
def findEncodings(imageList):
    encodeList=[]
    for img in imageList:
        img=cv2.cvtColor(img,cv2.COLOR_BGR2RGB)
        encode=face_recognition.face_encodings(img)[0]
        encodeList.append(encode)
    return encodeList
print("Encoding started")
encodeListKnown=findEncodings(imgList)
encodeListKnownWithIds=[encodeListKnown,studentIds]
print("Encoding Complete")

file=open("EncodeFile.p",'wb')
pickle.dump(encodeListKnownWithIds,file)
file.close()
```

Figure: 3.5



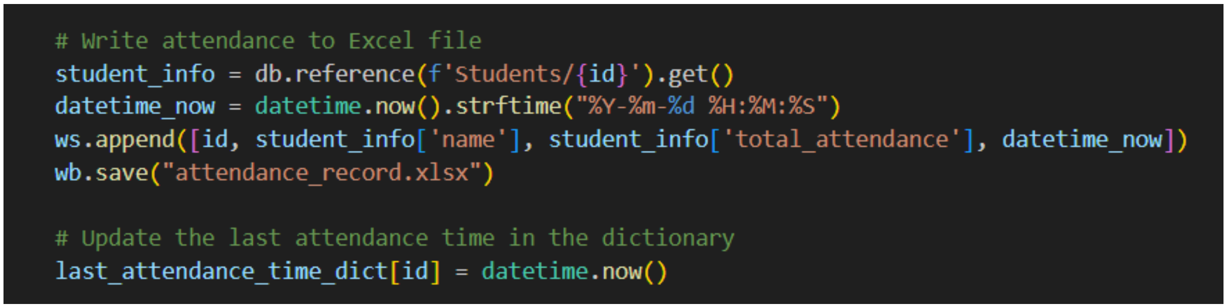
```
# Check if attendance can be marked
if can_mark_attendance(id):
    print(f"Attendance marked for ID: {id}")
    cvzone.putTextRect(imgBackground, "Loading", (275, 400))
    cv2.imshow("Face Attendance", imgBackground)
    cv2.waitKey(1)
    counter = 1
    modeType = 1

    # Write attendance to Excel file
    student_info = db.reference(f'Students/{id}').get()
    datetime_now = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
    ws.append([id, student_info['name'], student_info['total_attendance'], datetime_now])
    wb.save("attendance_record.xlsx")

    # Update the last attendance time in the dictionary
    last_attendance_time_dict[id] = datetime.now()
```

Figure : 3.6



```
data={
"321654": # in order to mark the attendace of the person, image name should be 321654.png same goes for all.
        {
            "name":"Manoj Mehta",
            "major": "cloud",
            "starting_year": 2020,
            "total_attendance": 6,
            "standing": "G",
            "year": 4,
            "last_attendance_time": "2024-5-11 00:54:34"
        },
"852741":
        {
            "name": "Samyak Pahalwan ",
            "major": "IT",
            "starting_year": 2020,
            "total_attendance": 12,
            "standing": "B",
            "year": 4,
            "last_attendance_time": "2024-5-11 00:54:34"
        },
```

Figure:3.7



```
# Write attendance to Excel file
student_info = db.reference(f'Students/{id}').get()
datetime_now = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
ws.append([id, student_info['name'], student_info['total_attendance'], datetime_now])
wb.save("attendance_record.xlsx")

# Update the last attendance time in the dictionary
last_attendance_time_dict[id] = datetime.now()
```

Figure :3.8

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.

Chapter 4: Testing

4.1 Testing Strategy

Testing Strategy:

- **Unit Testing:** Validate that each React component renders correctly and behaves as expected by testing them individually. Check if face-api.js functions result in expected outputs.
- **Integration Testing:** Ensure that the React components integrate with the face-api.js system.Make sure the library supports facial recognition well with the React.
- **End-to-End (E2E) Testing:** Simulating user interaction using E2E testing tools such as Cypress and Selenium. Start with a pilot test of the entire authentication process, starting from image capture and ending at successful log in.
- **Performance Testing:** Evaluate the performance of the system with different load configurations.Test the speed of facial recognition process.
- **Security Testing:** Assess the facial recognition model in relation to common attacks such as spoofing and replay attacks. Protecting the sensitive data such as the biometric information.
- **Usability Testing:** Evaluate the user feedback on the process of facial recognition. Ensure the system gives precise results after facial recognition tries.

Testing Tools:

1.Testing Framework:

- Jest: Widely used JS testing framework for testing of react apps.

2.Testing Utilities for React:

- React Testing Library or Enzyme: Assists in testing of React component interactions.

3.End-to-End Testing:

- Cypress or Selenium: For end-to-end testing, several of the E2E testing tools can be used to simulate users' interactions and test authentication processes as a whole.

4.2 Test Cases and Outcomes

Test Cases:

- **Testing of Components:** Check to see if React components render correctly. Examine the facial recognition-related user interface components.
- **Testing for functionality:** Check the face detection and recognition system's accuracy. Examine the results under various lighting conditions for false positives and false negatives.
- **Integrity Checking:** Make sure that face-api.js and React components integrate properly. Make sure information is transferred between components as it should be.
- **E-to-E Testing :**Play the role of a user trying to log in using facial recognition.After a successful recognition, confirm that the user's authentication was accurate.
- **Evaluation of Performance:** Test the speed of facial recognition for different image quality levels. Analyze the system's performance when several users are using it at once.
- **Testing for security:**Try to get around the system by employing common attacks or spoofing images.Make sure that unauthorized attempts are rejected by the system.
- **Testing for Usability:** Make sure the user gets understandable feedback when using facial recognition.In case of errors or failures in recognition, test the behavior of the system.

Outcomes:

- Success Scenarios:Facial recognition accurately authenticates users.React components work seamlessly with face-api.js.System performs well under expected loads.

- Issues/Defects:Incorrect facial recognition results. React components not rendering or functioning correctly. Security vulnerabilities, such as susceptibility to spoofing.

- Improvements: Enhancements to improve facial recognition accuracy. Optimizations for React component performance. Security patches for identified vulnerabilities.

Chapter 5: Results and Evaluation

5.1 Results

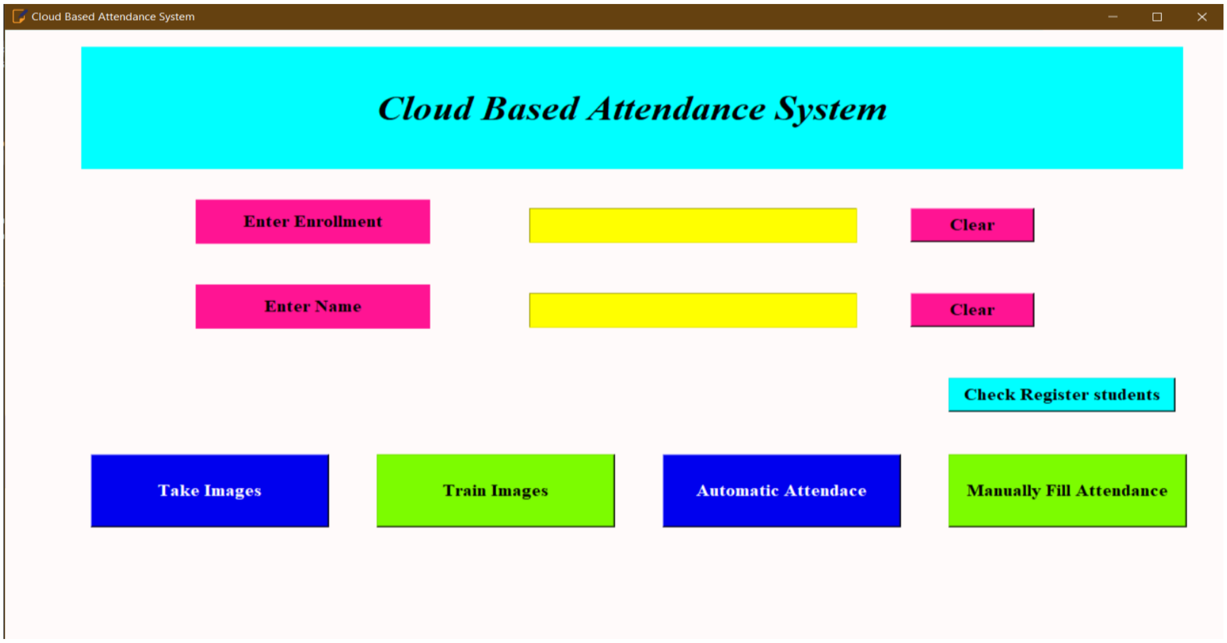


Figure:5.1

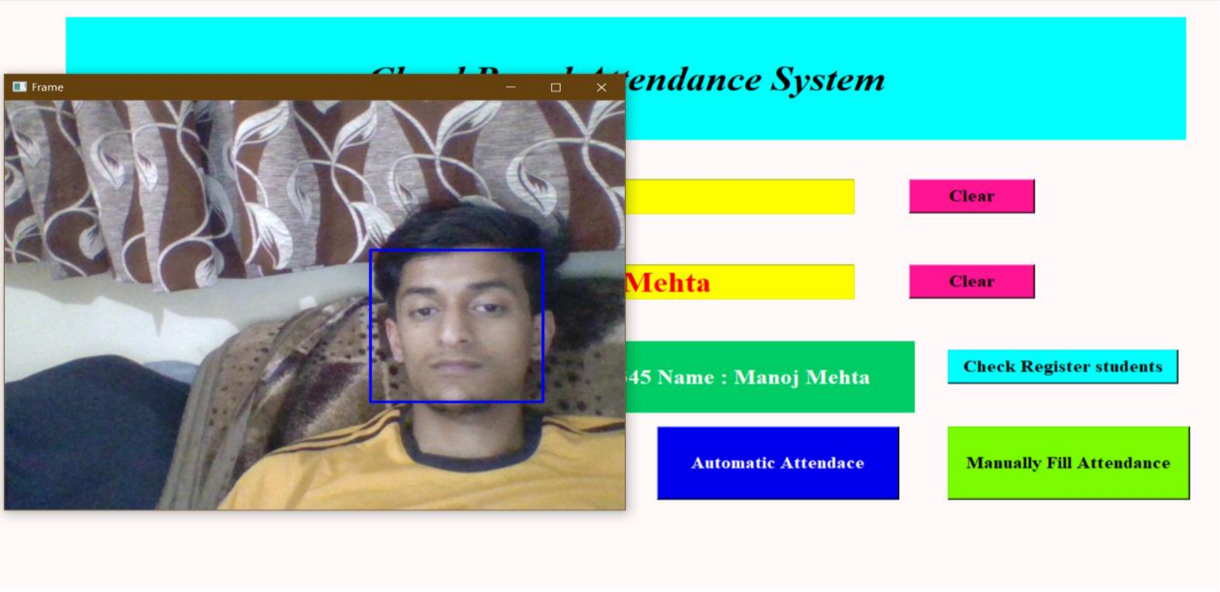
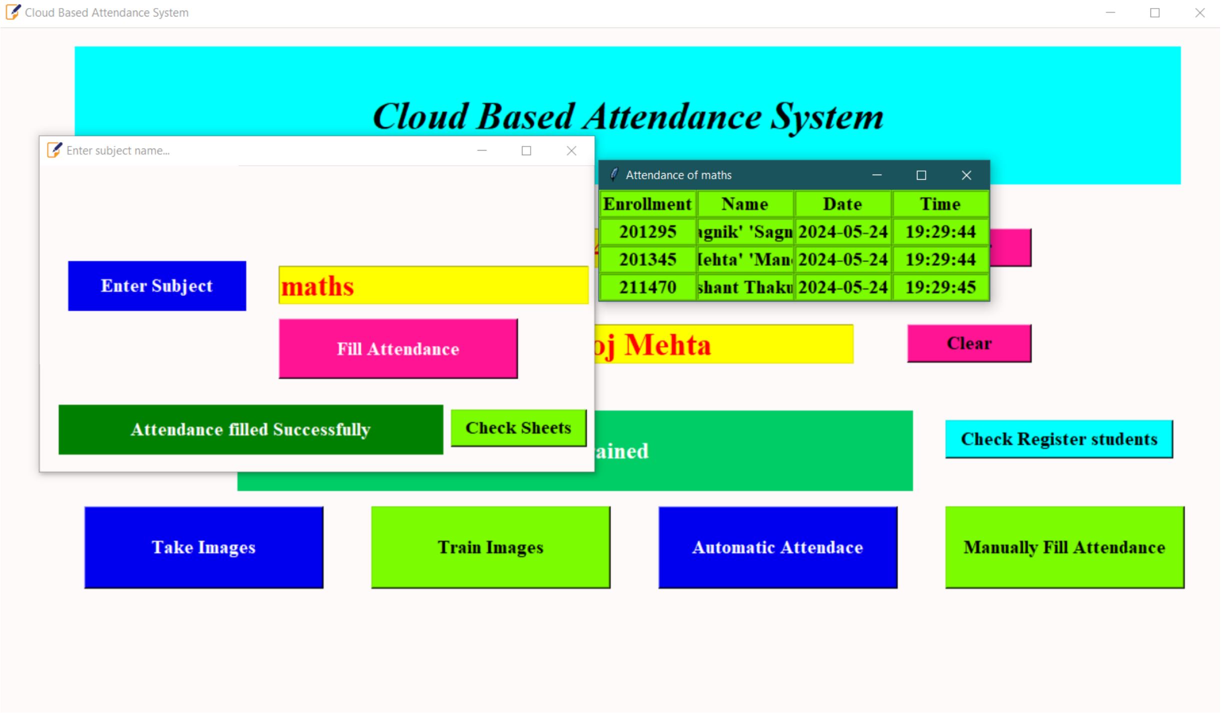


Figure:5.2



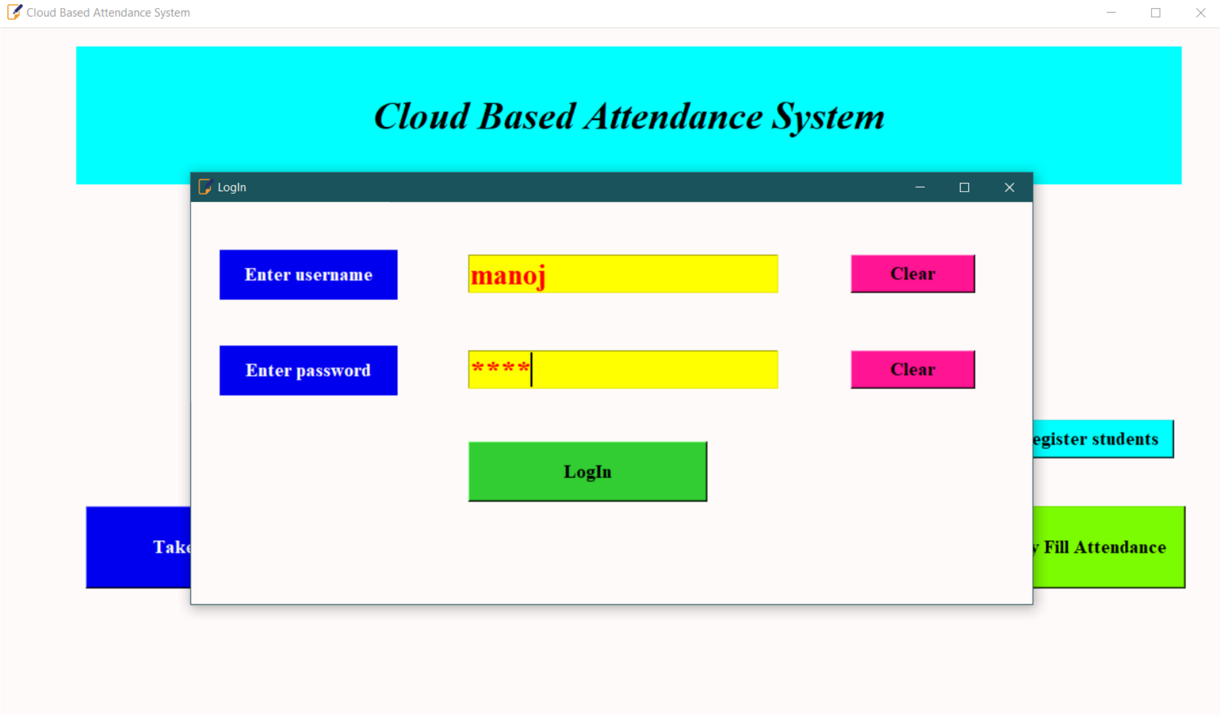
Enter Subject: maths

oj Mehta

Attendance filled Successfully

Enrollment	Name	Date	Time
201295	ıgnik' 'Sagn	2024-05-24	19:29:44
201345	lehta' 'Man	2024-05-24	19:29:44
211470	shant Thaku	2024-05-24	19:29:45

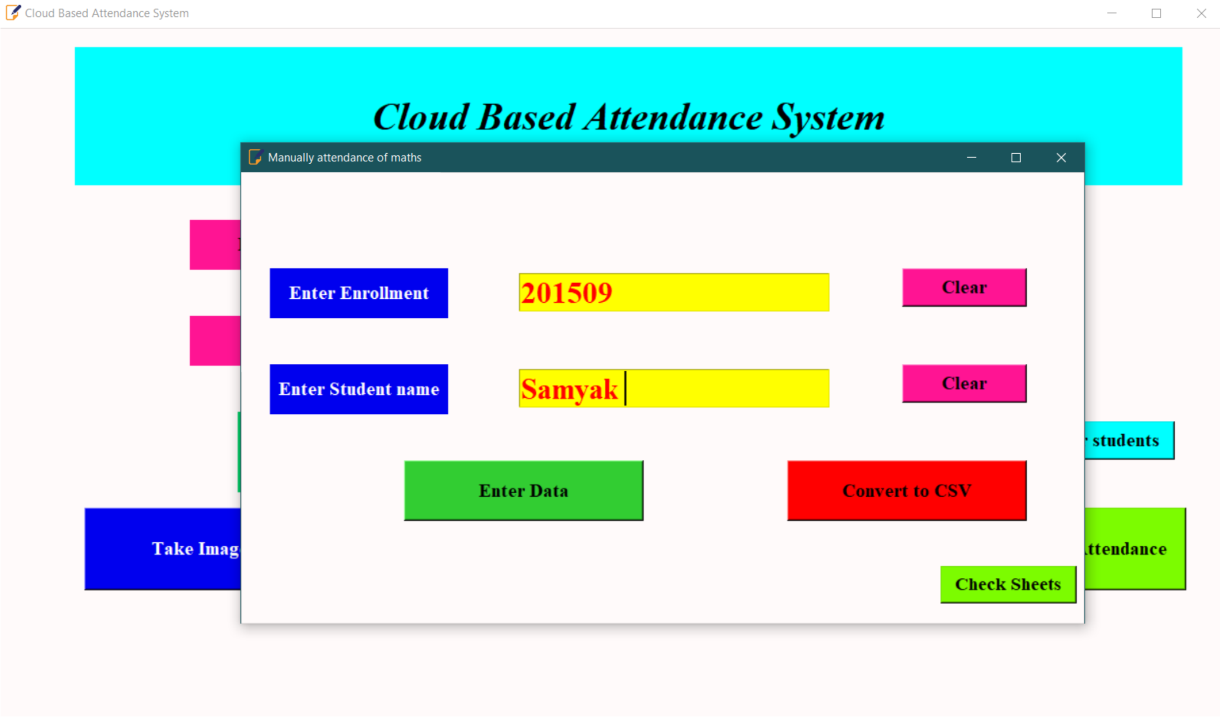
Figure: 5.3



Enter username: manoj

Enter password: ****

Figure :5.4



201509

Samyak

Figure:5.5

Chapter 6: Conclusions and Future Scope

5.1 Conclusion

In conclusion, the project on Cloud Based Attendance 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

- A voice recognition system, an iris scanner, and fingerprint technology will be added to the project to further improve its authentication capabilities. Apart from facial recognition, each modality provides distinct biometric data, giving users several safe options for authentication.

- A website that uses cloud-based storage is being developed,by which data will be more scalable and accessible. An increasingly connected and user-friendly experience can be achieved by storing user data in the cloud, which also makes data synchronization and persistence across multiple devices possible.

- The ongoing frontend development shows a commitment to enhancing the user interface and overall user experience. Improvement of the design, user interaction optimization, and the integration of responsive design principles to guarantee accessibility on various devices are likely to be the main components of frontend enhancements.

- The project now includes a hardware component as a result to the Arduino sensors integration. Sensors may improve user interactions or offer extra data inputs for authentication. Because of Arduino's flexibility, different sensors can be integrated, extending the project's potential beyond software-based authentication techniques.

- The importance of security and privacy highlights a dedication to safeguarding user information. To find and fix potential vulnerabilities, this could require placing strict access controls in place, implementing cutting-edge encryption techniques, and conducting frequent security audits. Placing an excessive value on privacy indicates that you understand how crucial it is to protect user data according to privacy laws.

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/

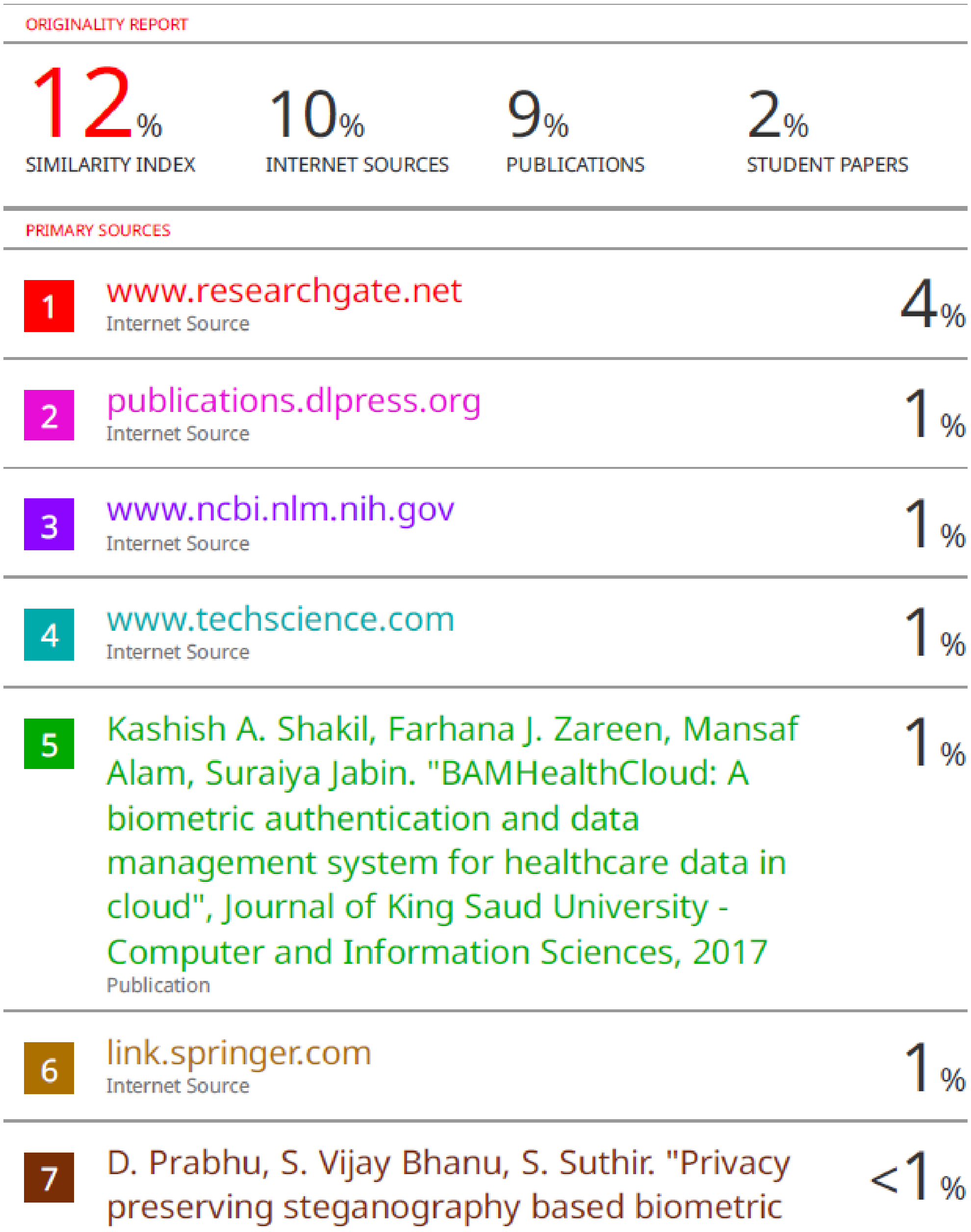
[20]. https://docs.docker.com/engine/security/

[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.

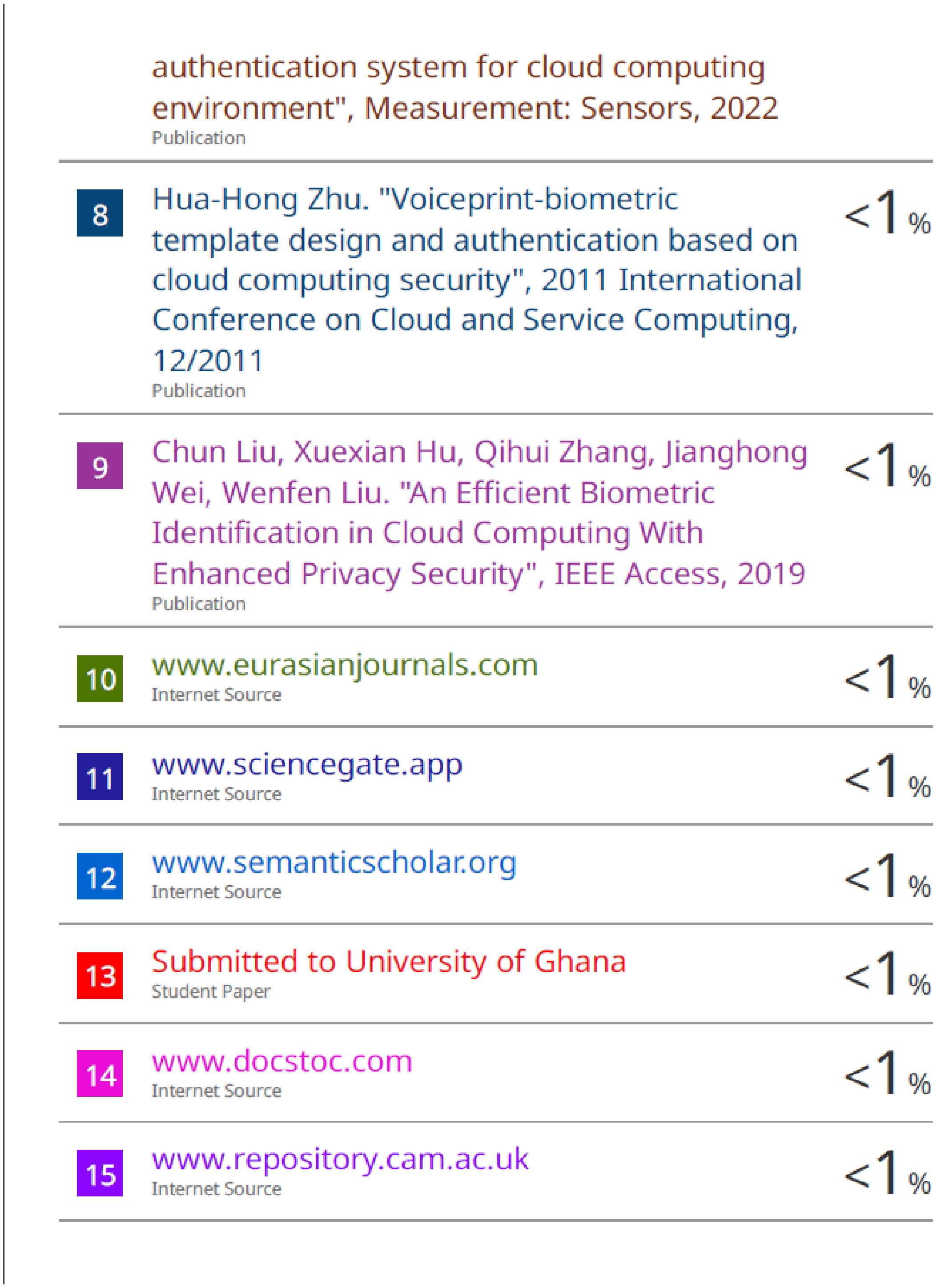


ORIGINALITY REPORT

12%	10%	9%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	4%
2	publications.dlpress.org Internet Source	1%
3	www.ncbi.nlm.nih.gov Internet Source	1%
4	www.techscience.com Internet Source	1%
5	Kashish A. Shakil, Farhana J. Zareen, Mansaf Alam, Suraiya Jabin. "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud", Journal of King Saud University - Computer and Information Sciences, 2017 Publication	1%
6	link.springer.com Internet Source	1%
7	D. Prabhu, S. Vijay Bhanu, S. Suthir. "Privacy preserving steganography based biometric	<1%



	authentication system for cloud computing environment", Measurement: Sensors, 2022 Publication	
8	Hua-Hong Zhu. "Voiceprint-biometric template design and authentication based on cloud computing security", 2011 International Conference on Cloud and Service Computing, 12/2011 Publication	<1 %
9	Chun Liu, Xuexian Hu, Qihui Zhang, Jianghong Wei, Wenfen Liu. "An Efficient Biometric Identification in Cloud Computing With Enhanced Privacy Security", IEEE Access, 2019 Publication	<1 %
10	www.eurasianjournals.com Internet Source	<1 %
11	www.sciencegate.app Internet Source	<1 %
12	www.semanticscholar.org Internet Source	<1 %
13	Submitted to University of Ghana Student Paper	<1 %
14	www.docstoc.com Internet Source	<1 %
15	www.repository.cam.ac.uk Internet Source	<1 %