CERTIFICATE AUTHENTICATION USING PERIOCULAR FEATURES

PROJECT PHASE - II REPORT

Submitted to the APJ Abdul Kalam Technological University

in partial fulfillment of requirements for the award of degree

Bachelor of Technology

in

Computer Science and Engineering

by

MUHAMMAD NIHAL M (MEE20CS024)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MES COLLEGE OF ENGINEERING AND TECHNOLOGY

KUNNUKARA

KERALA

APRIL 2024

MES COLLEGE OF ENGINEERING AND TECHNOLOGY,

KUNNUKARA

DEPT. OF COMPUTER SCIENCE AND ENGINEERING

2023- 24

CERTIFICATE

This is to certify that the report entitled **CERTIFICATE AUTHENTICATION USING PERIOCULAR FEATURES** submitted By **MUHAMMAD NIHAL M (MEE20CS024)** to the APJ Abdul Kalam Technological University in partial fulfillment of the B.Tech. degree in Computer Science and Engineering is a bonafide record of the project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Guide Head Of the Department

Internal Examiner External Examiner

ACKNOWLEDGEMENT

First and foremost, I would like to thank our greatest teacher of all: God. I know that I am here and that I’m able to write all of this for a reason.

I would like to express our gratitude to the management of MES College of Engineering and Technology, Kunnukara for providing us with all sorts of support for the completion of this project.

I record our sincere gratitude to our Principal **Dr. Preetha R Nair** for her guidance and sustained encouragement for the successful completion of this project.

I feel immense pleasure in expressing our humble note of gratitude to **Prof. K.M. Remesh**, Head Of the Department, Computer Science and Engineering, MES College of Engineering and Technology, Kunnukara as well as our Project coordinator **Dr. Noora V.T**., Associate Professor, Department of Computer Science and Engineering, MES College of Engineering and Technology, Kunnukara for their remarkable guidance and for offering incessant help in all possible ways from the beginning.

I express our profound sense of gratitude and heartfelt thanks to our project guide, **Mrs A Thilakavathi** , Assistant Professor, Computer Science and Engineering, MES College of Engineering and Technology, for her support and encouragement during the inevitable and often unpredictable crisis.Our heartfelt thanks for the expert guidance, constant encouragement, patience, passion and discipline that have been indispensable for our growth. Her motivating words, loving attitude and valuable suggestions had laid the foundation stone for building up this project.

Finally, I would like to extend our sincere thanks to all our beloved teachers and student friends for their constant support and encouragement the successful completion of the project.

ABSTRACT

This work “Certificate Authentication using Periocular Features” uses the unique patterns and features of the skin surrounding the eye, such as eyelids, eyelashes, eyebrows etc to recognize individuals. For example, the eyes of a human being have a greater than symbol and a less than symbol hidden in them. In every human being, there are almost 80 points that can be extracted and they are different for each individual. It’s considered as a subset of facial recognition technology, as the periocular region is a critical component of the face and contains important distinguishable features. The process of periocular recognition involves capturing a digital image or video of the periocular region, extracting unique features using computer algorithms, and comparing these features with pre-existing database of known individuals to identify a match. The network is trained on a collection of periocular images and their related ID’s. The network gains the ability to extract identifying the characteristics from these photos that are discriminative. By using this extraction method, we can apply for several certificate and many other purposes. In this after extraction certificates are generated.

Contents

List of Figures

Chapter 1

Introduction

In today's digital age, the authenticity and security of certificates play a pivotal role in various domains, including education, employment, and legal documentation. Also, in a fiercely competitive job market, the proliferation of fraudulent academic certificates poses a significant challenge. Traditional paper-based certificates are prone to forgery and tampering, leading to a growing demand for robust and efficient certificate authentication systems. Also, Traditional certificate authentication methods are time-consuming, leading to delays in verifying credentials. The usage of fake certificate is also increasing nowadays. Fake certificates and credentials can cause significant damage to universities and other educational institutions as it causes reputational damage, loss of accreditation, legal liability, financial loss, loss of prestige. Hence it is very important to make the verification process more accurate and secure [1]. This work proposes a certificate authentication mechanism using QR code. For this, primarily the image of the user is required. The unique eigen distances are then extracted from the periocular region. These eigen distances are hided into a QR code and this QR code is implemented in the certificate of the user. This QR code is encrypted using AES for enhancing the security of verification. For the verification process, this QR code need to be decrypted and the eigen distances stored in the QR code is matched with the eigen distances extracted from the image of the user. Hence the status of the certificate can be identified and the acknowledgement is sent to the user. This process reduces the use of fake certificates [1].

Chapter 2

Literature Review

In order to build a strong foundation and to obtain an idea about the feasibility of the project a number of resources were referred. Scholarly articles including published papers that are most relevant and significant to the topic have been included during the research period.

2.1 Periocular Recognition Based on Features from Thermal and Visible – Light Images

Periocular recognition is a biometric authentication method that uses the eye region, which remains relatively unchanged due to various factors such as poses, aging, and facial expressions. A method has been proposed that uses both visible-light and thermal images for periocular recognition, with the expectation that this approach will be robust against changes in illumination and facial expression. The method involves extracting features from the periocular region in both thermal and visible modalities, and then concatenating these features. A lightweight periocular recognition framework, named Masked Mobile Lightweight Thermo-visible Face Recognition (MmLwThV), has also been proposed. This framework uses thermo-visible features and an ensemble subspace network classifier to improve upon existing periocular recognition systems. The MmLwThV framework successfully improves accuracy over a single visible modality by mitigating the effect of noise present in the thermo-visible features. It is lightweight and can be easily deployed on mobile phones with a visible and an infrared camera [2]. Advantages of this paper is that it can identify a person while mask on face, is more accurate than only using visible light images and the disadvantages are equipment cost, accessibility and the lighting condition [2].

2.2 Combining Arc Face and Visual Transformer Mechanisms for Biometric Periocular Recognition

In recent years, biometric identification applications have become increasingly popular. This highlights the need for improved recognition techniques and more suitable biometric traits. Research has shown that attention mechanisms, which are crucial in biological vision systems including human vision, can significantly enhance the accuracy of recognition rates in computer vision systems. It has found that the periocular region is less affected by environmental changes compared to the entire face, achieving similar performance using just a quarter of the facial data. A new method for periocular recognition has been proposed. This method integrates attention mechanisms with a recent architecture known as Visual Transformer (ViT), along with the ArcFace loss function. Advantages are that it does not require direct interaction with the authentication system, it is less susceptible to variations in the environment than facial images and disadvantages are that it cannot handle spoofing attacks, requires a large amount of dataset. [3]

2.3 IoT Enabled Multimodal Biometric Recognition System in Secure Environment

Designing an IoT-enabled multimodal biometric recognition system in a secure environment involves integrating various biometric modalities such as fingerprint, facial, and iris recognition. The system comprises IoT devices equipped with biometric sensors, microcontrollers, and connectivity modules for data capture and communication. A central processing unit and an IoT gateway aggregate and process data before transmitting it securely to a cloud infrastructure. 2.3 IoT Enabled Multimodal Biometric Recognition System in Secure Environment [2] Certificate Authentication Using Periocular Features Dept of CSE MESCET,Kunnukara The cloud hosts a biometric database and authentication server, ensuring data integrity and enabling multi-factor authentication. Strong security protocols, encryption, and compliance with privacy regulations are paramount. The user interface should be user-friendly, and monitoring/logging mechanisms, along with regular updates and scalability considerations, contribute to a reliable and efficient system. Ethical considerations, energy efficiency, and adherence to regulatory standards are essential elements in the development of a robust and secure IoT-enabled multimodal biometric recognition system. Advantages of this papers are increased amount of individual data, reduce restriction of unimodal biometrics, frauds can be reduced and disadvantages are that it use lot of biometric methods / more complex, high cost for implementation [4]

2.4 Iris and Periocular Recognition using Shape Descriptors and Local Invariant Feature

ris and periocular recognition, employing shape descriptors and local invariant features, represent a cutting-edge approach to biometric identification. Iris recognition focuses on the intricate patterns within the iris, while periocular recognition extends the analysis to the surrounding eye region. Shape descriptors capture the geometric characteristics of these features, translating them into computationally digestible forms. Simultaneously, local invariant features enable the identification of key points within these regions, ensuring the system's adaptability to variations in lighting and imaging conditions. By combining the strengths of shape descriptors and local invariant features, this biometric system achieves a remarkable level of accuracy and resistance to fraudulent attempts, making it particularly well-suited for high-security applications such as access control and identity verification. properties of the iris and periocular regions. This integration of advanced image processing techniques ensures a robust and efficient biometric recognition system, capable of providing reliable identification in real-world scenarios [5].Advantages of this paper are high accuracy, uniqueness and robustness. Disadvantages are privacy concern, limited storage and cost.

2.5 M2FRED: Mobile Masked Face Recognition Through Periocular Dynamic Analysis

Mobile masked face recognition through periocular dynamic analysis represents an innovative solution to address challenges posed by the widespread use of face masks, especially in the context of mobile devices. Given that traditional face recognition may be hindered by mask-wearing, focusing on the periocular region — the area around the eyes — becomes crucial for accurate identification. This approach involves dynamic analysis of periocular features, taking into account subtle facial movements, blinking patterns, and unique characteristics of the eyes. By leveraging the mobility of smartphones and their built-in cameras, this system captures and analyzes periocular dynamics to provide a reliable and secure means of face recognition even when individuals are wearing masks [6]. Advantages are useful for security and authentication, partial face recognition, non-intrusive. Disadvantages are only possible for upper areas, limited accuracy, security concern.

Chapter 3

System Analysis

3.1 Feasibility Study

Feasibility study is a test of a system according to its workability, impact on the organization’s ability to meet user needs and effective use of resources. There are three aspects in the feasibility study portion of the preliminary investigation. [8]

- Technical Feasibility
- Economic Feasibility
- Software Feasibility
- Hardware Feasibility

3.1.1 Technical Feasibility

The technical requirements for the system are economic and it does not use additional software. That is whether the system can be implemented using the existing technologies or not. This project is platform independent since it is developed using python, whose development kit are easily available and free of cost, thus making the system technically feasible.[1]

3.1.2 Economic Feasibility

The proposed project is economically feasible. Because once the system is put into its use in the current market the system provides economical advantage to the firm, Also the firm can afford the cost to implement the project. This system doesn't need any initial investment and can improve the quality of service. The softwares used in this project such as AES, sublime, pycharm etc are free of cost.[1]

3.1.3 Software Feasibility

Even though this application is developed in very high software environment, it is also supported by many other environments with minimum changes. The system is fully feasible to be executed on any kind of operating systems and browsers.[1]

3.1.4 Hardware Feasibility

Software can be developed with the existing resources. But the existing resources may or may not be used to produce hardware if no hardware is newly bought for project, then software is said to achieve hardware feasibility. The system is hardware wise feasible because it doesn't need any new hardware other than the inbuilt camera in system.[1]

Chapter 4

Methodology

4.1 System Architecture

The system architecture shown in fig 4.1 depicts the various stages involved in the proposed work such as data collection, QR code generation, certificate generation and certificate verification. For the certificate generation process, the user primarily sends the personal information and photo to the authority. The authority does the eigen distance extraction from the periocular region of the image, convert the eigen distance into a QR code and the QR code is encrypted using AES. This QR code is implemented in the certificate and certificate is send to the user. For the certificate verification process, the user sends the certificate and image to the organization. They do the QR code decryption and the eigen distance extracted from this is made to match with the eigen distance extracted from the image. The acknowledgement regarding the status of the verification is send to the user. The 4 stages of the system architecture are explained below

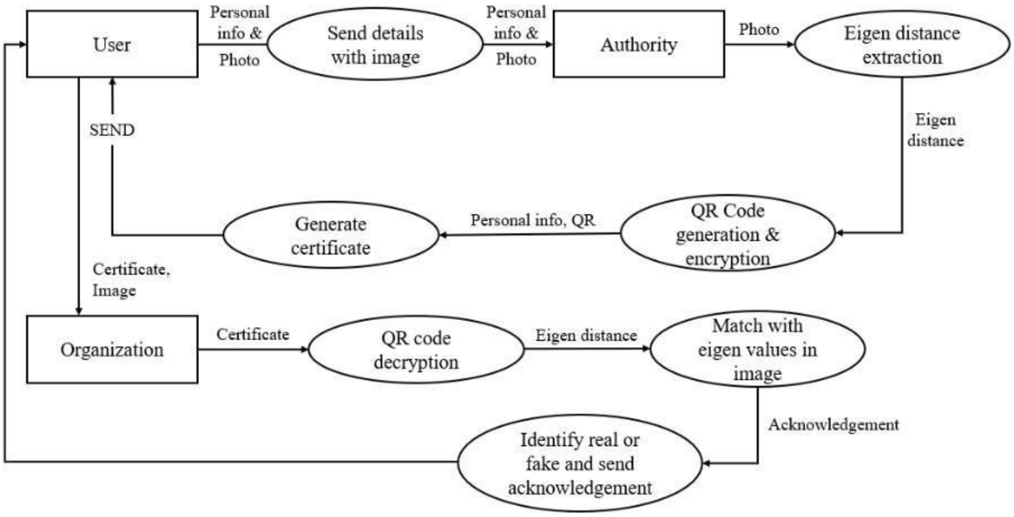


Figure 4.1: System Architecture

4.1.1 Data collection

In data collection phase, the image of users consisting of periocular region are collected for the purpose of certificate generation that includes eigen distance extraction and QR code generation. The images will be in the format of jpg.

4.1.2 QR code generation

n QR code generation phase, around 80 points in the periocular region are considered such as eyebrow, upper eyelid, eyeball etc and distance from these points to chin is measured. These distances are unique for each individual. These extracted values are converted into a QR code. This QR code encrypted using AES for improving security.

4.1.3 Certificate generation

After the QR code generation, containing the eigen distances extracted from the image of the user, this QR code is implemented in the certificate along with the personal information and other details. This final certificate is forwarded to the user.

4.1.4 Certificate verification

For the verification purpose, the user sends the certificate into the organization. The organisation primarily decrypts the QR code using AES and extract the eigen distances. These eigen distances are made to compare with the eigen distances extracted from the image of the user. If both are same, the certificate is declared to be real. Else, It is fake. Certificate verification can also be done as a single stage without the prior stages explained above.

4.2 Data Flow Diagram

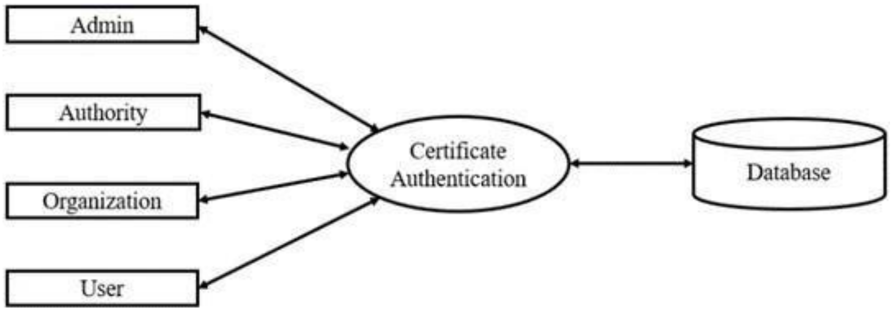


Figure 4.2: Level 0

Admin

Admin has the overall control over the web application. Authority and Organization should primarily register under the Admin.

Authority

Authority is the one who generate the certificate. User need to send his personal information along with an image for the purpose of QR code generation and certificate generation.

Organization

Organization is the one who need to verify whether the certificate is real or fake through the process of QR code decryption, eigen value extraction and matching.

User

User is the one who need to get the certificate generated. User send their details to the authority for certificate generation

Database

Database is where the data from the admin, authority, organization and user are getting stored.

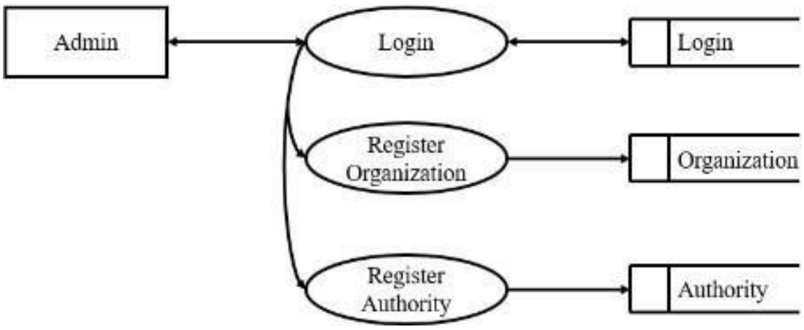


Figure 4.3: Level 1

Register Organization

The organization needs to register under the admin for the further procedures using a username and password. This username and password will be used for further logins.

Register Authority

The Authority needs to register under the admin for the further procedures using a username and password. This username and password will be used for further logins.

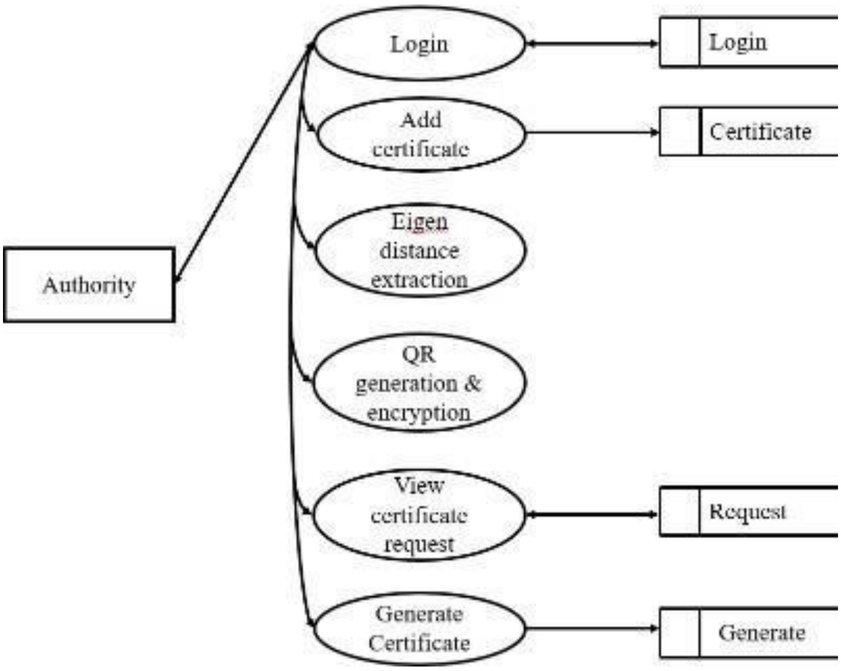


Figure 4.4: Level 2

Login

Primarily, authority needs to login using the username and password used for registration. After login only authority can do the procedures of certificate generation.

Add certificate

Add certificate means adding the name of the certificates that are issued by the authority. This is done by the authority and the available modes of certificates can be viewed by the user.

Eigen distance extraction

Eigen distances are extracted by taking distance between nearly 80 points and chin. These distances are unique for each individual.

QR generation and encryption

These eigen distance are hided in a QR code and it is encrypted using AES for security. This QR code is implemented on the certificate.

View certificate request

Authority can view the request send by the user for the generation of certificate. Each request will be having a generate button. Clicking it will generate the certificate.

Generate certificate

Authority is the one who generate the certificate. Clicking the ‘generate’ button shown with each request will generate the certificate.

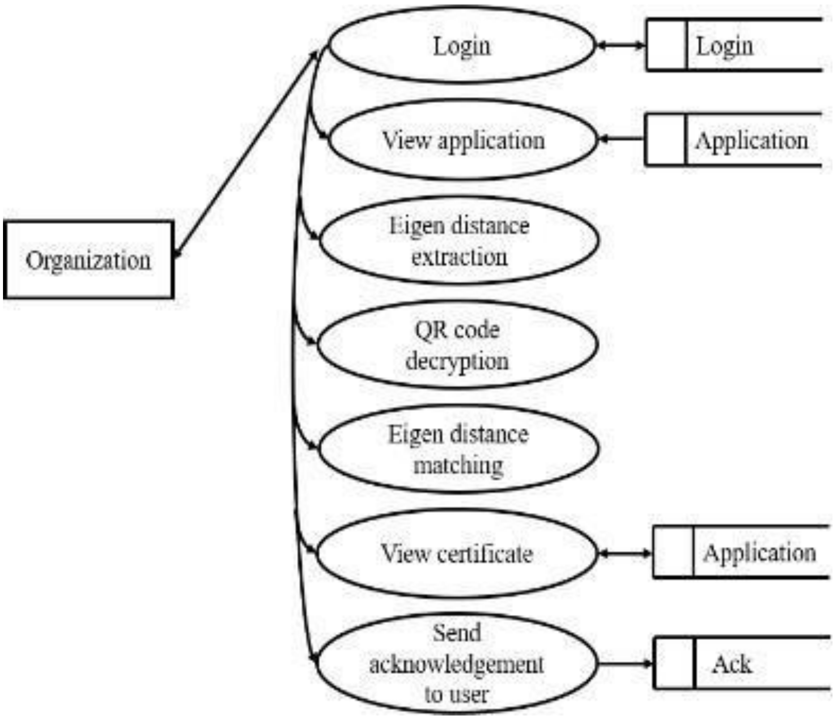


Figure 4.5: Level 3

Login

Organization can view the application along with the certificate send by the user for certificate verification.

View application

Organization can view the application send by the user for certificate verification.

Eigen distance extraction

Organization also does the eigen distance extraction from the image of the user for finding a match with eigen distance in the QR code.

QR code decryption

The QR code need to be decrypted using AES before the matching process due to security policy.

Eigen distance matching

The eigen distance extracted by the organization from the image of the user is compared with the eigen distance provided in the QR code.

View certificate

The organization can view the certificate send by the user for verification.

Send acknowledgement to user

Organization sends acknowledgement to the user regarding the status of the certificate after verification process, ie, whether the certificate is fake or real.

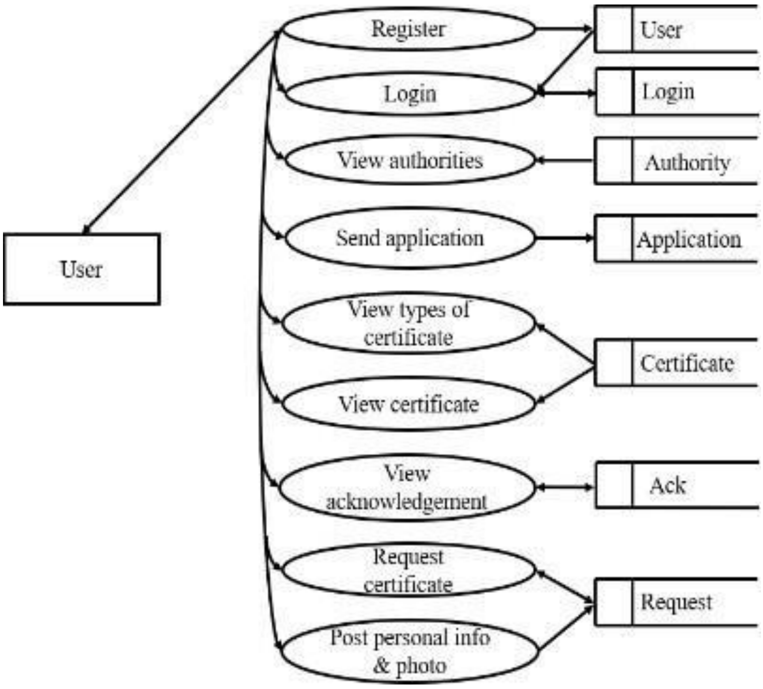


Figure 4.6: Level 4

Register

If the user is new to this web application, he/she needs to do registration using a username and password.

Login

If he/she is already a registered user, they will have to login using the username and password used for registration for further procedures.

View authority

User can view the different authorities registered under the admin and can select under which authority they need to get the certificate generated.

Send application

The user can send application to the organization for certificate verification.

View types of certificate

User can select which type of certificate they need to get generated.

View certificate

User can view the generated certificate send to them by the authority.

View acknowledgement

User can also view the acknowledgement on the status of verification process send by the organization.

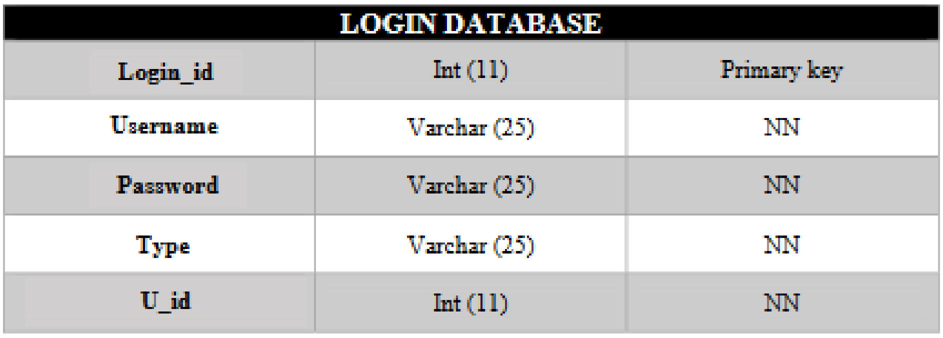
Request certificate

The send the request to the authority along with their personal information and photo to the authority for the generation of their certificate.

4.3 Database Schema

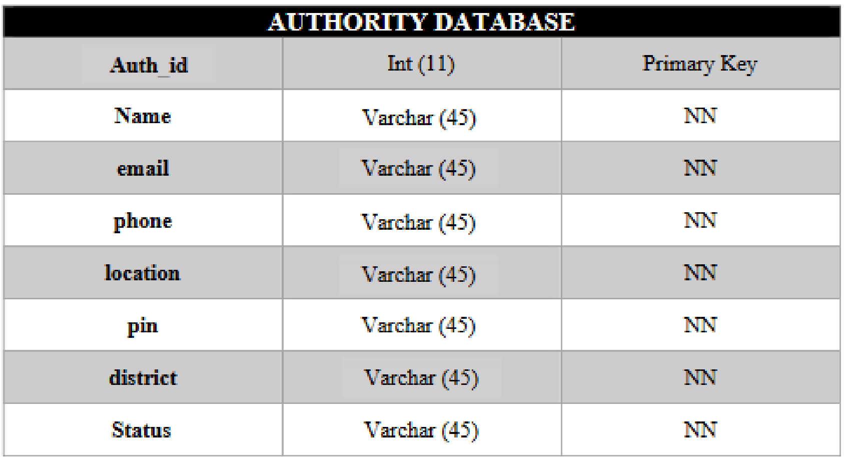
The proposed system requires the use of numerous databases. The basic schema of the databases are shown below:

The login database in figure 4.3.1 holds information about the user's credentials to verify and authenticate successful login in to corresponding pages. It stores password as a hash value for security and uses as login id as a primary key.



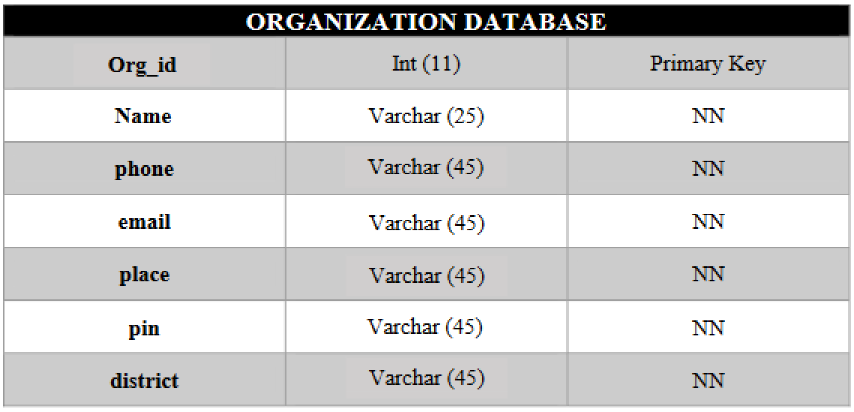
LOGIN DATABASE		
Login_id	Int (11)	Primary key
Username	Varchar (25)	NN
Password	Varchar (25)	NN
Type	Varchar (25)	NN
U_id	Int (11)	NN

Table 4.3.1: Login Database Schema



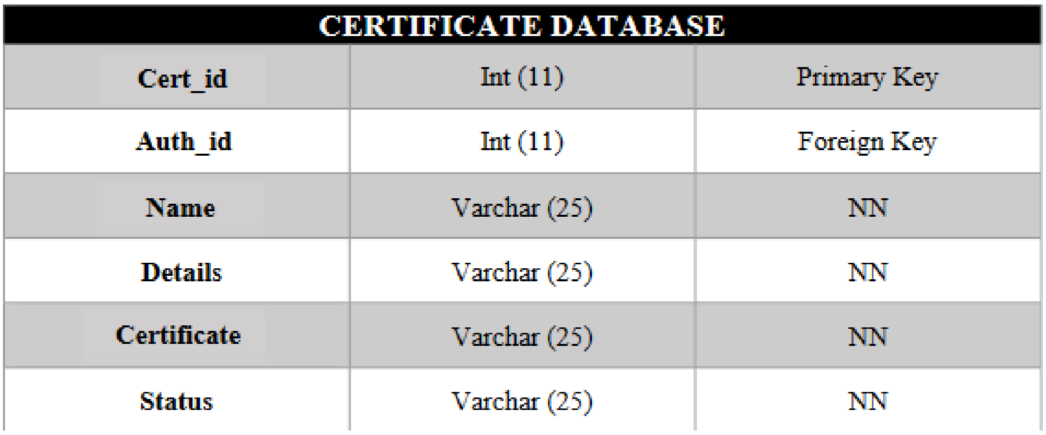
AUTHORITY DATABASE		
Auth_id	Int (11)	Primary Key
Name	Varchar (45)	NN
email	Varchar (45)	NN
phone	Varchar (45)	NN
location	Varchar (45)	NN
pin	Varchar (45)	NN
district	Varchar (45)	NN
Status	Varchar (45)	NN

Table 4.3.2: Authority Database Schema



ORGANIZATION DATABASE		
Org_id	Int (11)	Primary Key
Name	Varchar (25)	NN
phone	Varchar (45)	NN
email	Varchar (45)	NN
place	Varchar (45)	NN
pin	Varchar (45)	NN
district	Varchar (45)	NN

Table4.3.3: Organization Database Schema

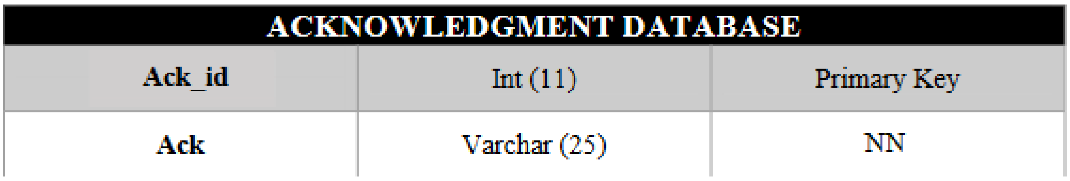


CERTIFICATE DATABASE		
Cert_id	Int (11)	Primary Key
Auth_id	Int (11)	Foreign Key
Name	Varchar (25)	NN
Details	Varchar (25)	NN
Certificate	Varchar (25)	NN
Status	Varchar (25)	NN

Table4.3.4: Certificate Database Schema

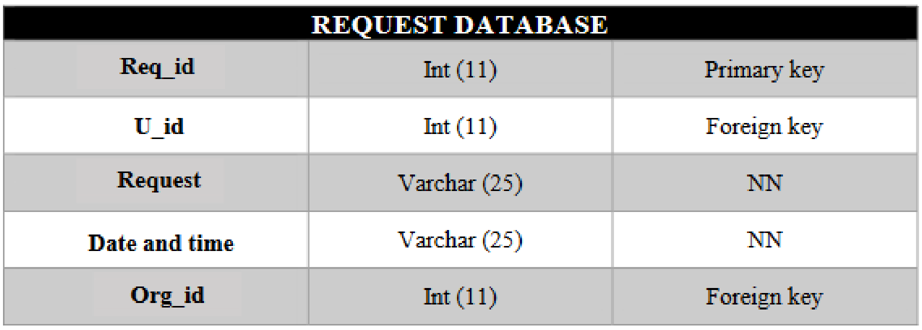
The authority database in figure 4.3.2 holds information of the user to generate certificate Primarily, authority needs to register under the admin for entering the authority page and later on, they have to login using the username and password (email) for further procedures. Authority id is the primary key.

The organization database in figure 4.3.3 holds information of user to verify the certificate. Primarily, organization needs to register under the admin for entering the organization page and later on, they have to login using the username and password (email) for further procedures. Here, organization id is used as primary key.



ACKNOWLEDGMENT DATABASE		
Ack_id	Int (11)	Primary Key
Ack	Varchar (25)	NN

Table4.3.5: Acknowledgement Database Schema



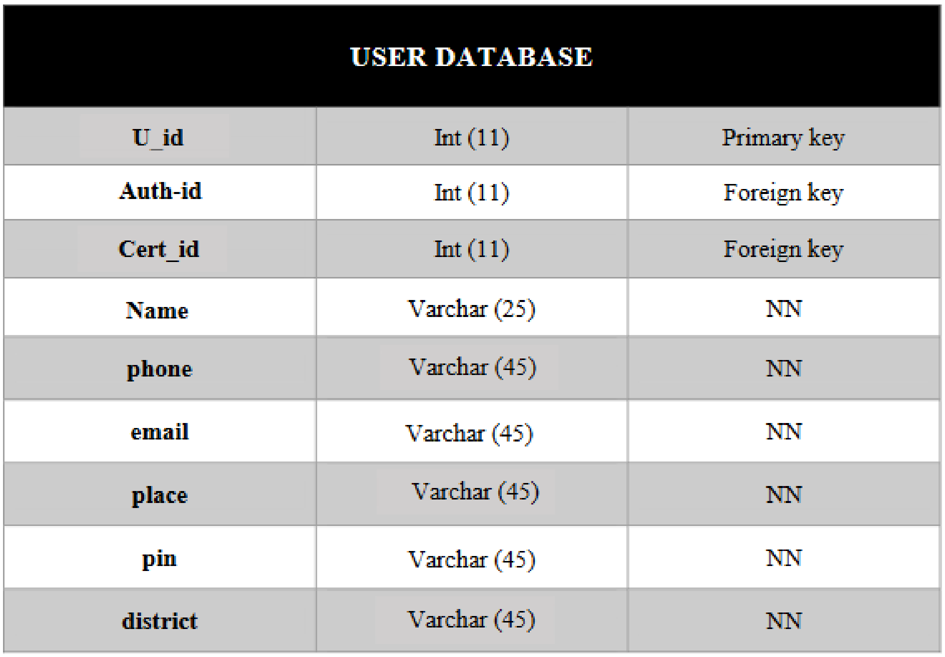
REQUEST DATABASE		
Req_id	Int (11)	Primary key
U_id	Int (11)	Foreign key
Request	Varchar (25)	NN
Date and time	Varchar (25)	NN
Org_id	Int (11)	Foreign key

Table4.3.6: Request Database Schema

The certificate database in figure 4.3.4 holds information about which type of certificate they need to get generated. Certificate id is used as primary key and authority id is used as foreign key.

The acknowledgement database in figure 4.3.5 holds the acknowledgements. After verification, organization send acknowledgment to user on the status of verification, ie, whether the certificate is real or fake. Organization sends acknowledgement and user views this acknowledgement. Here, acknowledgement id is used as primary key.

The request database in figure 4.3.6 holds the requests send by the user. User can send request to authority for generation of certificate and to organization for the verification purpose. Here, request id used as primary key. User id and organization id is used as foreign key



USER DATABASE		
U_id	Int (11)	Primary key
Auth-id	Int (11)	Foreign key
Cert_id	Int (11)	Foreign key
Name	Varchar (25)	NN
phone	Varchar (45)	NN
email	Varchar (45)	NN
place	Varchar (45)	NN
pin	Varchar (45)	NN
district	Varchar (45)	NN

Table4.3.7: User Database Schema

User database in figure 4.3.7 holds the information of user. Primarily, user needs to register under the admin for entering the user page and later on, they have to login using the username and password (email) for further procedures. User id is used as primary key. Authority id and certificate id is used as foreign key

Chapter 5

System Design and System Implementation

As discussed in the design phase of the project, since the project involves operations that are extremely varying and different from each other, the same programming tools cannot be used. So, the best and most efficient tools to perform each task were sought out in the implementation phase and integrated together. How each of these operations were implemented are conferred about in the upcoming sections.

5.1 Periocular feature extraction

Periocular recognition focuses on identifying individuals by examining the region around the eyes like eyelashes and jaw to eyebrows and almost all part of the face. This method is valuable for biometric identification, especially when facial recognition is impractical due to obstructions like masks, sunglasses, or veils. In certificate authentication, periocular recognition adds a layer of security by verifying the identity of the person presenting a certificate. The process begins with capturing quality images of the periocular region, followed by pre-processing to improve quality and isolate the region. Feature extraction, a critical step, involves analyzing texture, shape, color, or utilizing deep learning models like convolutional neural networks (CNNs) to identify unique patterns. Periocular points are marked from feature extraction and are hided in a QR code. These distances are then matched against a image of the user to determine if there’s a match, leading to a final decision on authentication.

5.2 Eigen value calculation

Eigenvalue calculation in the context of certificate authentication using periocular feature extraction involves identifying the key characteristics of the periocular region by analyzing

numerical representations of this area. The process starts with the collection and pre-processing of periocular images from a diverse set of individuals. These images are transformed into eigen vectors, which are used to create a eigen matrix. Eigenvalues and eigenvectors are extracted from this matrix. The eigenvalues indicate the variance explained by each eigenvector, with larger eigenvalues representing greater importance. The principal components derived from the eigenvalue calculation allow for a reduction in the dimensionality of the feature space while retaining critical information. This technique is crucial in certificate authentication, where these principal components can be used to train machine learning models or build databases for verifying identity. When a certificate is presented, the periocular features are extracted and transformed using the same principal components, allowing a comparison with stored patterns to confirm authenticity. This approach provides a reliable and efficient means of authenticating individuals based on periocular characteristics, a key aspect of many security applications.

5.3 QR code and certificate generation

The QR code serves as a machine-readable representation of this information, allowing for quick scanning and data retrieval. When implementing QR codes for certificate authentication, the QR code is generated by hiding the extracted eigen distances to the QR code and encrypting it[9]. This QR code is displayed in the certificate along with details of the user. This generated certificate[10] can be downloaded by the user. For the implementation in a periocular recognition-based certificate authentication project, the QR code can be embedded directly on the certificate or provided as a separate authentication key. When a certificate is presented, an authorized scanner reads the QR code to retrieve the encoded data. This data can be cross-checked with the image of the user to ensure the certificate's authenticity. Additionally, when combined with periocular recognition, the QR code can link to a database where periocular features of authorized individuals are stored, allowing for a multi-factor authentication process.

5.4 Encryption and decryption of QR code

Encryption and decryption of QR codes[11] play a pivotal role in ensuring that the information encoded within these codes remains secure and accessible only to authorized individuals. This is especially important in security-related applications such as certificate authentication using periocular recognition. To encrypt a QR code, sensitive data is first converted into an encrypted format using algorithms like Advanced Encryption Standard (AES) or Rivest–Shamir–Adleman (RSA), depending on whether symmetric or asymmetric encryption is employed. Once encrypted, the data is transformed into a QR code, which can be scanned and decrypted by those with the correct decryption key. In the context of certificate authentication, this approach adds an extra layer of security, ensuring that only those with the right credentials can access the encrypted information within the QR code. This not only protects against unauthorized access but also supports multi-factor authentication, where the decryption process is combined with periocular recognition to confirm the identity of the certificate holder. Such measures enhance security, protect sensitive information from tampering, and ensure the reliability of certificate-based systems.

5.5 Certificate verification

Verification of a certificate[12] in a project involving certificate authentication using periocular feature extraction involves a multi-faceted process to ensure both the authenticity of the certificate and the identity of the person presenting it. This process begins with an examination of the certificate itself, checking for QR codes that contain encoded information about the certificate’s origin and validity. When the certificate is presented, a biometric scan of the periocular region is performed to capture unique features such as eyebrows, eyelids, and surrounding skin. These extracted periocular features are transformed into numerical representations and compared with stored biometric data associated with the certificate in a secure database or referenced through the QR code. If the comparison yields a match, the certificate is declared to be real and the individual is verified as the rightful holder. This dual-layer approach verification, combining traditional certificate checks with advanced biometric recognition, provides robust security against fraud or impersonation. This method of certificate verification offers a reliable and secure solution for authentication in various applications, enhancing both security and confidence in certificate-based systems.

5.6 Database Tables

The proposed system requires the use of numerous databases. The databases were created in MySQL Workbench 8.0 to facilitate the storage and management of tables. Without these tables the functionality of the forms cannot be Implemented.

5.6.1 Login Table

The login table holds details of each login occurred through the home page using the POST method. No additional method to update the table is required.

5.6.2 Authority Table

The Authority table contains details of authority who has registered under the admin using POST method.

5.6.3 Organization Table

The Organization table contains details of organization who has registered under the admin using POST method.

5.6.4 Acknowledgement Table

The acknowledgement table holds the acknowledgements send by the organizations using POST method on the status of the verification.

5.6.5 Request Table

The Request table holds the requests send by the user for the certificate generation.

5.6.6 Certificate Table

The certificate table holds information about the types of certificates being issued and other details related to it.

5.6.7 User Table

The user table contains the username and other details like their phone number, admission number etc.

5.7 Web Application

There are mainly two reasons why the project was decided to be developed in the form of a web application:

1. It is not restricted to a single operating system. If the application had to be expanded to be compatible with other operating systems in the future, a web application seamlessly allows this to happen.
2. Takes up very little storage and requires less processing power. Since the testing and evaluation phase has to be done in an online virtual environment where storage and processing power is limited, this was the most viable option.

Figure 5.1: Home page

5.7.1 Home Page

The login pages consist of both user registration and the login page. This was made to be simple yet aesthetically pleasing. The login page contains a username and password for login purpose. The username used during registration is taken as the username and the email used during registration is taken as the password. This login page can be used by authority, organization and user. After entering the required login information, the webpage takes you to the directed page. A PHP script that incorporated HTML and CSS in the front end was developed for all pages. A logout button is provided in each page which takes you back to this home page.

5.7.2 Admin Page

The admin page contains the registration form for organization and authority. The username and passwords used during the registration will be used for further logins.

CERTIFICATE AUTHENTICATION
USING PERIOCULAR FEATURES

Figure 5.2: Admin page

AUTHORITY POINT

Figure 5.3: Authority page

5.7.3 Authority Page

The Authority page is specifically designed to cater to the needs of authorities involved in the project. This page includes options such as ‘view request/Generate certificate’ for viewing the request send by the user for generation of certificate and generate the certificate[10] including the QR code[9] by clicking the generate button present along with each request. An ‘add certificate’ option is provided for adding different types of certificates being issued by authority.

Figure 5.4: Organization Page

5.7.4 Organization Page

The Organization page is specifically designed to cater to the needs of organizations involved in the project. This page contains options such as ‘send acknowledgement’ for sending the status of verification to the user as the organization does the verification process, ‘verify’ for verifying whether the certificate is real or fake by comparing the eigen distances from image and the QR code and a ‘view request’ for viewing the applications send by the user.

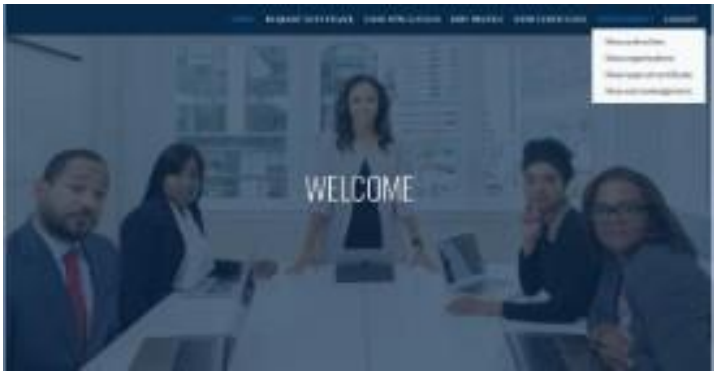


Figure 5.5: User Page

5.7.5 User Page

The user page is specifically designed to cater to the needs of users involved in the project. This page contains options such as ‘Send Application’ for sending the application to the organization for verifying certificate, ‘Request Certificate’ for sending request to the authority for certificate generation,‘View authorities’ for viewing which all authorities are available, ‘View organizations’ for viewing which all organizations are available, ‘View types of certificate’ to view which all types are being issued by the authority, ‘View certificate’ for viewing the certificate generated, “Edit profile’ for editing the current user profile and ‘View acknowledgement’ for knowing the status of the verification.

Chapter 6

Testing and Result

The experimentation of ‘Certificate Authentication using Periocular Features’ has been a compelling area of exploration, showcasing the potential of this technology to revolutionize the traditional certificate verification model. Several experiments and projects have emerged, demonstrating the advantages and novel features authentication using periocular features can offer.

6.1 Results

Periocular Feature Extraction: The periocular region refers to the area around the eyes, including the eyelids, eyebrows and surrounded area. After getting the image being send by the user, periocular points are marked from the image by the authority as shown in fig 6.1. then eigen distances are extracted using these points. These extracted eigen distances are encrypted into a QR code as shown in fig 6.2 and is encrypted using AES.

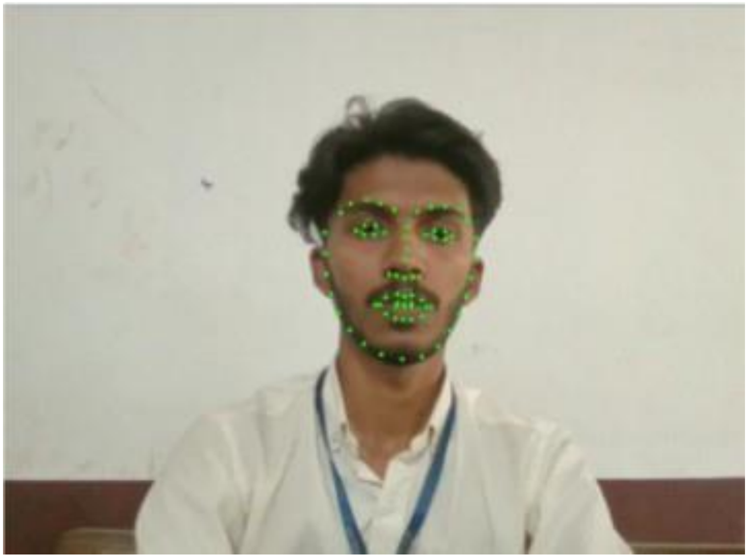
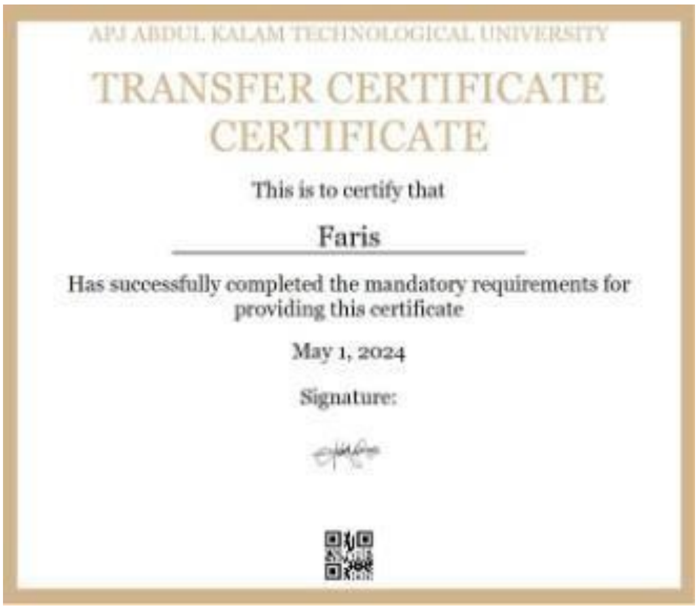


Figure 6.1: Periocular points extraction

Figure 6.2: QR code generation



APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

TRANSFER CERTIFICATE
CERTIFICATE

This is to certify that

Faris

Has successfully completed the mandatory requirements for providing this certificate

May 1, 2024

Signature:

Figure 6.3: Certificate generation

Certificate Generation: The authority generates a certificate of the user as per the request the receive. The name of the user along with the type of certificate they need to get generated, name of the authority, signature of authority head and the generated QR from the image is provided in the certificate as shown in figure 6.3. After the generation of the certificate, it is sent to the user. The user can view the same and download it in pdf format.

Certificate verification: This module of the project is carried out by the organization. After receiving the request from the user along with the certificate, the organization compares the eigen distance decrypted from the QR code and the eigen distance extracted from the image of the user as shown in fig 6.4. If these distances match, the certificate is declared to be real as shown. Else it is declared to be fake. An acknowledgement regarding the verification is sent to the user.

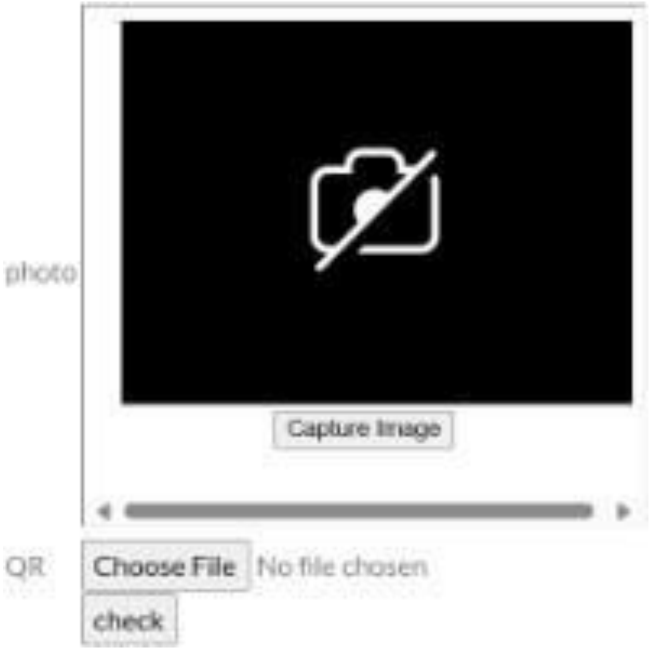


Figure 6.4: Verification

6.2 Evaluation

The evaluation of our project has shown promising results. Primarily, the transparency offered by this work enables the users to have a clear view of how the certificate is generated and how verification is done. A number of images of different individuals are used for analyzing the performance of the proposed system. Periocular features are extracted from each of these images. An image is compared to all the other images. In an ideal case no two images should match. And it is to be checked that whether the matching images (images of the same person) are shown as unmatched by the system, for this, images of the same person is selected and one of them is compared with all the other images, in such a case an ideal system should never declare the images as unmatched. In related projects, the area around the eye

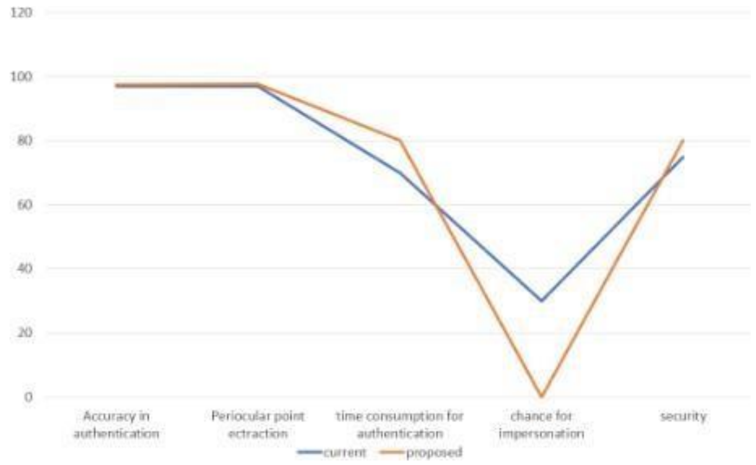


Figure 6.5: Comparison graph

alone was used for periocular recognition purposes. But in this work, the distance from the area around the eye to different points on the face were extracted. The project offers 98recognition which is higher comparing the current recognition mechanisms. The time for certificate authentication is also less for this project when compared to the existing methods. Only a single QR code and an image of the user is required for authentication purpose [9]. Impersonation wont work this project because the QR is generated from the image of the user. The values in a QR generated for a particular user cannot be altered by a third party since it is encrypted[11]. Security is more in this mode of authentication because AES is used for encryption and decryption[11]. The graph comparing existing technology and proposed methodology is shown in fig 6.5

Chapter 7

System Requirements

7.1 HTML

The Hyper Text markup Language or HTML is the standard markup language for documents designed to be displayed in a web browser. Web browser receive HTML documents from a web browser or from local storage and render the documents into multimedia web pages. HTML describes the structure of a webpage semantically and originally included cues for the appearance of the document. In our project its used for front end of web application and provide a structure for it.

7.2 CSS

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language such as HTML.CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript.CSS is designed to enable the separation of presentation and content, including layout, colours, and fonts.

7.3 Django

Django is a powerful Python-based web framework. Django uses a model view template architecture which helps to making the development process more organized and efficient [8]. Django gives a flexible authentication process. Learning Django would be relatively easy. This can help to speed up the development process. In this project, it is used for web development.

7.4 MySQL Workbench

MySQL supports SQL, a standard language for managing and manipulating databases. This allows users to create, modify, and extract data from the relational databases. MySQL is compatible with numerous platforms like Microsoft Windows, Oracle Solaris, AIX, Symbian, Linux, MAC OS. In this project, it helps to store the different data.

7.5 PyCharm

Pycharm is a powerful and versatile python IDE. It's designed to provide all the tools you need for productive python development. It supports SSL and SSH configuration which helps for certificate authentication. Pycharm also provide its own storage for trusted certificate [8]. It offers great framework-specific support for modern web development frameworks such as Django, Flask, Google App Engine, Pyramid, and web2py. All the codes related with the project are stored in Pycharm.

Chapter 8

Future Scope and Conclusion

The project "Certificate authentication using periocular features" can reduce the use of fake certificates in various fields. In this project, a new mode of certificate verification is established. The work primarily extracts the unique features from the periocular region of the user and eigen distances are calculated. A QR code containing the eigen distances of the periocular region of the user is attached into the certificate along with the personal information and other details of the user. This certificate can be viewed and downloaded by the user. This is the certificate generation process. This QR code is encrypted using AES for safety. This work also includes the certificate verification phase. Comparing the value in the QR code to the eigen distance extracted from the image of the individual can make the organisation understand whether the certificate is real or fake. The organisation sends acknowledgement regarding the status of verification to the user. Future works can include expanding this authentication for IoT devices, web applications, mobile devices and cloud services.

References

[1] Ms Srivika S, Ms Gayathri L, Ms Nivetha B, Ms Sri Devi N and Mrs Sujatha R, *“Biometric Verification using Periocular Features based on Convolution Neural”*, Karur, India, Year 2023

[2] Andrea Francesco Abate, Lucia Cimmino, Immacolata Cuomo, Mario Nardo, and Teresa Murino. *”On the impact of multi-modal and multi-sensor biometrics in smart factories”*IEEE Trans. on Industrial Informatics, 2022

[3] P. Kumari and K. R. Seeja, *“A novel periocular biometrics solution for 935 authentication during COVID-19 pandemic situation”* J. Ambient Intell. 936 Humanized Comput., vol. 12, no. 11, pp. 10321–10337, Nov. 2021.

[4] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, *“Arcface: Additive angular margin loss for deep face recognition,”* in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4690– 4699, 2019.

[5] Zhao, Z. Kumar, A., *Improving Periocular Recognition by Explicit Attention to Critical Regions in Deep Neural Network”, I*EEE Transactions on Information Forensics and Security, vol. 13, no. 12, pp. 2937-2952, 2018

[6] Shangfei Wang et al *“Analyses of a multimodal spontaneous facial expression database for expression recognition and emotion inference”*IEEE Transactions on multimedia 12, 2010.

[7] ttps://www.sciencedirect.com/science/article/pii/ S1319157818313302

[8] Kishore,P.M.and Srinivas.K.(2015). *”certficate authentication usingPeriocular feature”* In Procedia Computer Science.45.765-772.

[9] Damon L. Woodard, Shrinivas J. Punlik, Jamie R. Lyle and Phillip E. Miller, *”Periocular Region Appearance Cues For Biometric Identification”* , IEEE, 2010.

[10] Kiran B. Raja, P. Raghavendran and Christoph Bush, *”Biometric recognition of Surgically Altered Periocular Region: A Comprehensive Study.”*

[11] Zhifeng Li, Unsang Park *”Discriminative Model for age Invariant Face Recognition”*,IEEE, 2011

[12] Muhammad Uzair, Arif Mahamood and Ajmal Mian, *”Periocular Biometric Recognition Using Image Sets”*IEEE, 2013.

[13] Farheen Sultana, Bikiran and Shobana, *” A Study On data Encryption Using AES And RSA”*

[14] L.Woodard,J.Punlik Jamie R.Lyle Philip E.Miller *”Periocular Region. Identification Appearance ”*987-1-5244-7030 IEEE 2010

[15] Kiran B.Raja, P. Raghavendran, Christoph Bush *”Biometric recognition of Surgically Altered Periocular Region: A Comprehensive Study”*

[16] Anil K Jain *”A Discriminative Model for age Invariant Face Recognition ”* 2011.

[17] Kang Roung Park, You Jin Ko *”Fake iris detection method using purkinje image based on gaze position”*,june 2008

[18] Sarp Erturk *”Nonintrusive iris image extraction* for iris recoginition.*based biometric identification”*,june 2006

[19] Yangsheng Wang,Xiaxio Zhou *”Real time detection of eye corners and iris center from image acquired by usual camera”*,march 2010

[20] Kumiko Tsuji , Miki Aoyagi *”Eye direction by stereo image processing using corneal reflection on an iris”*, january 2006

Appendix

Code

```
CREATE DATABASE  IF NOT EXISTS `sample` /*!40100 DEFAULT CHARACTER SET latin1 */;

USE `sample`;

-- MySQL dump 10.13  Distrib 8.0.31, for Win64 (x86_64)

--

-- Host: localhost    Database: sample

-------------------------------------

-- Server version    5.7.40-log


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;

/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;

/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;

/*!50503 SET NAMES utf8 */;
```

```
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;

/*!40103 SET TIME_ZONE='+00:00' */;

/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS,
UNIQUE_CHECKS=0 */;

/*!40014 SET
@OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS,
FOREIGN_KEY_CHECKS=0 */;

/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE,
SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;

/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0
*/;



--

-- Table structure for table `user`

--



DROP TABLE IF EXISTS `user`;

/*!40101 SET @saved_cs_client     = @@character_set_client */;

/*!50503 SET character_set_client = utf8mb4 */;

CREATE TABLE `user` (

  `U_id` int(11) NOT NULL AUTO_INCREMENT,

  `Name` varchar(25) NOT NULL,
  `Auth_id` int(11) NOT NULL,

  `Cert_id` int(11) NOT NULL,

  `Phone` varchar(25) NOT NULL,

  `Email` varchar(25) NOT NULL,

  `Place` varchar(25) NOT NULL,

  `Pin` varchar(25) NOT NULL,

  `District` varchar(25) NOT NULL,

  `admission number` varchar(45) NOT NULL,

  `age` varchar(45) NOT NULL,

  `image` varchar(45) NOT NULL,

  PRIMARY KEY (`U_id`)

) ENGINE=InnoDB DEFAULT CHARSET=latin1;

/*!40101 SET character_set_client = @saved_cs_client */;


--

-- Dumping data for table `user`

--


LOCK TABLES `user` WRITE;

/*!40000 ALTER TABLE `user` DISABLE KEYS */;
```

```
/*!40000 ALTER TABLE `user` ENABLE KEYS */;

UNLOCK TABLES;

/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;


/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;

/*!40014 SET
FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;

/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;

/*!40101 SET
CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;

/*!40101 SET
CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS
*/;

/*!40101 SET
COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION
*/;

/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;


-- Dump completed on 2024-03-21 14:00:38
```