Online-Journals.org

iJOE International Journal of
Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 19 No. 17 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v19i17.42635

PAPER

Iris Recognition Approach for Preserving Privacy in Cloud Computing

Nalini M K(✉), Preetha S, Sumedha Samanta, Tejaswini V, Yashasvi M

B.M.S. College of Engineering, VTU, Bengaluru, India

nalini.ise@bmsce.ac.in

ABSTRACT

Biometric identification systems involve securing biometric traits by encrypting them using an encryption algorithm and storing them in the cloud. In recent decades, iris recognition schemes have been considered one of the most effective biometric models for identifying humans based on iris texture, due to their relevance and distinctiveness. The proposed system focuses on encrypting biometric traits. The user's iris feature vector is encrypted and stored in the cloud. During the matching process, the user's iris feature vector is compared with the one stored in the cloud. If it meets the threshold conditions, the user is authenticated. Iris identification in cloud computing involves several steps. First, the iris image is pre-processed to remove noise using the Hough transform. Then, the pixel values are normalized, Gabor filters are applied to extract iris features. The features are then encrypted using the AES 128-bit algorithm. Finally, the features of the test image are matched with the stored features on the cloud to verify authenticity. The process ensures the privacy and security of the iris data in cloud storage by utilizing encryption and efficient image processing techniques. The matching is performed by setting an appropriate threshold for comparison. Overall, the approach offers a significant level of safety, effectiveness, and accuracy.

KEYWORDS

biometric, iris, authentication, Hough transform, Gabor filter, AES, cloud

1 INTRODUCTION

Many organizations are transitioning from traditional passwords to biometric authentication as a means of verifying identity. This is because traditional passwords are susceptible to data breaches. According to the *2019 Verizon Data Breach Investigations Report*, passwords accounted for 81% of data breaches. Biometric authentication, on the other hand, recognizes a person by using one or more morphological or behavioral characteristics, such as the iris, finger veins, or fingerprints, making it more difficult to replicate or forge. Biometrics outperforms traditional passwords in terms of accuracy, non-repudiation, and permanence. Certain challenges,

Nalini, M.K., Preetha, S., Samanta, S., Tejaswini, V., Yashasvi, M. (2023). Iris Recognition Approach for Preserving Privacy in Cloud Computing. *International Journal of Online and Biomedical Engineering (iJOE)*, 19(17), pp. 33–50. https://doi.org/10.3991/ijoe.v19i17.42635

Article submitted 2023-06-27. Revision uploaded 2023-09-27. Final acceptance 2023-09-27.

however, arise as biometric devices mature. For example, when enlistment rates are high, the computational and matching complexity increase, leading to higher prices and increased data storage requirements. A solution to this problem involves migrating the biometric module to the cloud. To reduce costs on storage and computation, the owner of the information, such as the FBI, may wish to transfer the vast amounts of biometric information to a cloud server. However, in order to protect the privacy of biometric data, it must be encrypted before being outsourced.

When an FBI partner, such as a police station, needs to verify a person's identity, they contact the FBI and initiate a search for the person's identity using their characteristics. The FBI then secures the inquiry by encrypting it before sending it to the cloud in search of a close match. This process ensures that biometric data is kept secure and private while also enabling the efficient and effective use of the system. The use of secure biometric template protection techniques is another important aspect of privacy-preserving biometric identification. These techniques are designed to prevent the unauthorized use of biometric information by creating a secure template of the biometric data that can only be accessed by authorized parties. This can include techniques such as biometric cryptosystems, which use encryption to protect the biometric data, and biometric watermarking, which embeds a digital signature into the biometric data to prevent tampering. It is also crucial to consider the legal implications of biometric data. Biometric data is considered sensitive personal information, and several countries have laws in place to protect it. India's Personal Data Protection Bill (PDPB) is one such example. These laws establish specific requirements for obtaining, storing, and using biometric data, and organizations must adhere to them. To summarize, privacy-preserving biometric identification in cloud computing is a crucial research field that seeks to safeguard individuals' privacy while their biometric data is stored, processed, and shared in cloud computing environments. Data encryption, secure protocols, and secure biometric template protection techniques can all work together to preserve biometric data and keep it safe from unauthorized access and use.

2 LITERATURE SURVEY

Santosh Kumar et al. [1] focused on privacy issues arising from cloud security. It provides a solution using biometric face recognition. The approach was broken down into three key stages.

1. **Acquisition of face images:** At this stage, face images are captured using sensors such as cameras. The Viola-Jones algorithm is used for locating and recognizing facial features in pictures.
2. **Extracting and pre-processing face features:** In order to accurately depict facial characteristics, the original face photos are cropped and resized to a standard resolution of 200 × 200 pixels in this phase. With further processing, these photos are used to extract distinctive facial traits, such as the shape of the eyes, nose, and mouth, which are then transformed into feature vectors.
3. **Recognition of individuals using encrypted biometric features:** Collected feature vectors are used to create specialized face templates and compared with those stored in a cloud-based face database. The suggested method secures data by employing two different encryption processes, namely Paillier and Elliptic Curve. The Euclidean distance algorithm is used to compare the encrypted features of facial photographs with a saved database. The proposed solution has

several restrictions, even though it can protect the privacy of data stored in the cloud. Tiny databases may not work effectively, as matching encrypted face characteristics consumes more time.

Salem et al. [2] presented a new technology that utilizes homomorphic encryption. A set of elements is mapped to another set using the mathematical notion of homomorphism, which ensures that mathematical procedures on the source set are preserved on the target set. The suggested system, known as Deep Zero ID, alters delicate biometric data while preserving the connections between the components. The system also took advantage of transfer learning, a method that utilizes a pre-trained deep neural network instead of training one from scratch using sensitive biometric data. A true-false detector is installed on the user's end to further enhance security. The extracted deep features were utilized by this detector to build a support vector machine (SVM) capable of distinguishing between genuine and counterfeit biometric data. With this method, studies revealed that it can verify integrated iris and biometric feature vectors with a 95.47% F1 score and zero false positives. Chun Liu et al. [3] proposed a novel method that makes use of the features of orthogonal matrices as well as additional randomization. It consists of three stages: preparation, request, and identification. There are three distinct entities: users, cloud servers, and data owners. The owner of the data has a database containing a vast amount of biometric information, including reference templates for individuals who have registered in the system. Using Finger Code, a baseline format vector is acquired from consumers during the preparation step and registered with the data owner. A secret key is then used to expand the vector and encrypt it. After encryption, the encrypted templates are sent to a cloud server. The data owner receives a user's identity request during the request stage and enhances it with an encryption key. The data owner then transmits the encrypted request to a cloud server. Each request is enhanced during this phase by adding security elements and random positive real integers. A request for identification is received by the cloud server during the identification step, and the server determines how closely the encrypted templates match the received request. A request is turned down if the relative distance is less than 0. According to the outcomes of the aforementioned strategy, it requires less computational complexity and provides more security. It was deemed appropriate for use with large databases.

Hui Zhu et al. [4] proposed an online fingerprint authentication scheme called e-Finga, which aims to be efficient and protective of user privacy. The method used 2DNF, an enhanced homomorphic encryption system that is comparable to the Paillier encryption system. The three components of the system are the trustworthy authority (TA), the Internet service's online authentication server (OASer), and the customers. The TA is responsible for encrypting and storing user-provided fingerprint templates. OASer receives the user's registration data and requests TA for relevant encrypted templates. Ciphertext is subsequently subjected to the matching criteria of OASer without decoding it. The matched results are then decoded by the account holder. Users can obtain trustworthy and secure fingerprint identification using the suggested method without revealing their fingerprints. This benefits users by protecting their privacy, as their sensitive biometric data remains encrypted and inaccessible to unauthorized parties. A biometric authentication system that utilizes the Microsoft Cognitive Face API in the cloud was proposed by Ashok Kumar B. Halvi et al. [5]. A facial image was taken as part of the system, and Dropbox was utilized to store it. The Microsoft Cognitive Face API was used to retrieve facial characteristics such as expression, gender, age, and facial key points. This was done after receiving a URL generated by Dropbox. The information was encrypted using advanced encryption standard (AES), a block cipher that utilizes symmetric keys to secure 128-bit data blocks. The encrypted data was then stored back in Dropbox. along with user data, was then stored back in Dropbox. Similar to the registration process, the verification procedure involves using a user-provided key and AES decryption to open the user's encrypted image that was registered. The Cognitive API receives verified, decrypted photos and authenticates them. The proposed system achieved 100 registered user face pictures and Aadhar photographs, with an accuracy rate of 96%.

In [6], a biometric identification system resistant to cloud collusion attacks was presented. Finger codes are first encrypted and uploaded to the cloud as a tuple containing an identification number. Finger codes are extracted from the fingerprint image during the identification step and encrypted before being sent to the cloud in the identification step. The user is authenticated if the Euclidean distance satisfies the threshold conditions. The authors compared their method with two other approaches and discovered that the proposed method consumed less time in both the preparation and identification processes. V. S. Nair et al. [7] proposed a new framework for authenticating users when uploading files to the cloud, which is supported by multimodal biometric cryptosystems. When logging in, the system considers the user's iris and fingerprint. Following that, the feature extraction module receives the collected biometric data. Iris code features are subjected to linear discriminant analysis to reduce dimensionality and eliminate code redundancy. After this process, the binary iris features are extracted. Data is transferred from the client to the server by providing the IP address of the server that is intended to receive the data. Data is transmitted to the server, where multi-biometric images composed of various biometrics are reconfigured. The server module utilizes a fuzzy vault to store the minutiae, which serves as the primary representation of the fingerprint. The polynomial degree of the fuzzy vault is selected to maximize the security of the system as well as the genuine acceptance rate (GAR). Though the attacker is aware of the iris features of a known user, it was only possible to achieve a security level of 35 bits. However, when there were no restrictions imposed on the fingerprint modality, the GAR was 70%, as opposed to 15%.

In [8], a system was proposed that enhances security by combining the AES algorithm with an AI-based artificial neural networks (ANN). Initially, the user provides a username and password, which are encrypted with AES and stored in a database. Iris recognition and fingerprint recognition are two biometric identification methods that can be chosen by the user. Biometric features are extracted using neural network algorithms and stored in the database. During the matching process, the user enters a username and password, which are then compared with the template stored in the database. Upon successful completion, the user will be subjected to biometric verification. If the iris or fingerprint (as selected by the user) matches the one in the database, the login is successful; otherwise, an error message is displayed. AES's performance accuracy was found to be 94%. A novel deep learning and cloud-based biometric system was proposed by T. Sudhakar et al. [9]. Cancellable biometrics have been utilized to address concerns regarding the privacy of biometric data stored in the cloud. In order to prevent spoofing and replay attacks during template transmission, a novel approach combining biometric cross-folding and QR code embedding was utilized. Initially, data is captured and cross-folded using a random matrix. A QR code is embedded in this cross-folded image and is sent to the cloud, where it is decoded. The AWS cloud platform runs the deep learning model. To extract features, CNNs are used, which transform the extracted biometric features into cancellable templates using random projection. For user authentication, an authentication module, which utilizes a multi-layer perceptron model (MLP), is hosted on the cloud platform. The approach achieved a validation accuracy of 80% on the MMU dataset, and on the FV-USM dataset, the accuracy was 92%.

H. Djalal Rafik et al. [10] suggested a biometric database for identification or authentication purposes. High-resolution digital cameras are required to capture high-quality iris photos. To segment the images, the Hough transform is used. The images are normalized, and Gabor filters are employed to extract features. Hamming distance was used to calculate the distance between the vectors during data matching. If the hamming distance is found to be higher than or equal to 0.5, the user is not authorized. The respective false acceptance ratio (FAR), false rejection ratio (FRR), and energy efficiency ratio (EER) values for the CASIA V1 database are 0.0363, 0.0374, and 0.05. The total accuracy is 99.9236%. FAR, FRR, and equal error rate of the MMU1 database, on the other hand, are 0.2425, 0.3407, and 0.3082, respectively. The overall accuracy is 99.4168. Changhee Hahn et al. [11] have addressed the two primary challenges related to efficiency and client privacy in biometric identification systems. Efforts were made to ensure that the process of identification consumes limited time and that only individuals have access to their biometric data. The proposed strategy incorporates the computational power of the cloud to handle most of the intensive calculations, thereby reducing the burden on the cloud service provider. The scheme includes three main components: client, server, and cloud. Since there are chances that an attacker may eavesdrop on the biometric data sent by the client or the cloud, in collusion with an external third party, and collect a client's biometric information for illegal gain, the scheme ensures client privacy through the use of symmetric homomorphic encryption. The scheme has three main steps. During the enrolment of the initial client, the client encrypts their finger code with a random key. Then the server encrypts the file again with its own key pair and sends it to the cloud. Finally, all three parties establish a secure connection to conduct a basic key exchange protocol. During the subsequent client enrollment, the second client encrypts the biometric data using a randomly generated key and sends it directly to the cloud. After performing a series of computations using the new key pair on the server, the cloud revises the entire biometric database using the new key. Once the database is updated, the cloud establishes a secure connection to refresh its key. This entire process is repeated for "n" clients. In the final step of secure biometric identification, the cloud calculates the Euclidean distances between the test data and the biometric database. The outcome is then encoded using the cloud's private key. Once the outcome is decrypted, the distance between the two finger codes is obtained. The cloud calculates all distances, chooses the shortest distance, and transmits it to the server, which uses a threshold to verify whether or not the client is authentic. The proposed scheme was developed using Java on an Amazon EC2 cloud-based Linux instance [20]. Results indicated relatively comparable performance during the enrollment phase compared to Yuan's scheme, but it requires less time during the identification phase, thus outperforming Yuan's scheme in terms of efficiency. In spite of several clients conspiring with the cloud, the combined key of vindictive clients does not have the potential to enable the cloud to infer biometric information of clients, nor can it obtain the server's key pair by any means. Xiaoping Yang et al. [12] have proposed a method that guarantees the confidentiality of user identification requests and datasets held by the service provider, while also maintaining a manageable level of computational resources required for cloud servers for biometric database searching. The main aim was to reduce the computational load on the cloud, which would otherwise have to parse through the entire biometric dataset to match an identification request. This process can be time-consuming, especially when there is a large number of identification requests to be served or when the dataset size is extensive. The scheme increases efficiency by using FITing tree and iDistance data structures, which reduce the search space during the identification process. The suggested scheme comprises a cloud consisting of two servers (CS1 and CS2), a client and a service provider. Two cloud servers are from separate cloud providers and they collaborate to process biometric identification requests. CS1 handles identification requests, saves the encrypted data set and indexes it. On the other hand, CS2 stores the confidential key and assists CS1 in obtaining identifications by decrypting the interim outcomes. Both servers possess strong computing power and ample storage capacity. The recommended scheme has four phases. In the first phase, the service provider establishes system parameters, including protection and authentication parameters, and delivers them to both the cloud servers and the client. During the second phase, the iDistance index is computed for each of the biometric templates in the dataset, and a FITing-tree is constructed using these indexes. The service provider then uses symmetric homomorphic encryption to encrypt the dataset, searching index (reference points), and outsources them to CS1 along with FITing-tree segments and maximum distance list. In the third phase, the client uses symmetric homomorphic encryption to generate an encrypted request for identification that corresponds to a particular biometric reference. In final phase, the encrypted authentication request generated in the previous phase is transmitted to CS1. Two cloud servers collaborate to obtain and provide the identification results to the client. When comparing the proposed scheme with MASK (by evaluating the synthetic dataset and the Labeled Faces in the Wild (LFW) dataset), the former has a lesser running time when it comes to encrypting indexes, a lesser identification time when the dataset grows, a lesser communication and storage cost, and better accuracy.

P. Punithavathi et al. [13] suggested a system wherein a cloud-based cancellable biometric system operates as a client-server framework. The system consists of a cancellable biometric template database and a processing engine residing on a cloud-based server, with a sensor unit placed on the client side. The processes of enrollment and verification of biometrics act as application programming interfaces that connect the user's device to the cloud. The sensor unit captures the user's iris biometrics and sends them to the cloud for enrollment with the assistance of the cloud controller. Feature extraction components derive relevant characteristics from the input picture of the iris. Later, the random matrix generation unit produces a random matrix and assigns a specific slot number to it. The feature transformation unit applies a matrix to the iris features, and the resulting data is stored in a cloud database. The slot number is then provided to the user for use in the verification stage. During verification, the feature transformation unit applies the same matrix (using the slot number input by the user) to the input features, generating a query template. The matching component on the cloud server utilizes a query template and previously stored transformed features at a specific slot to determine if there is a match. It outputs a "yes" or "no" based on the probability of the comparison. The proposed system was tested on a cluster computer comprising 12 servers and 78 cores, utilizing the CASIA and IIT Delhi Iris databases. The system achieved high identification accuracy rates of 94.31% for the CASIA dataset and 95.27% for the IIT Delhi Iris database. The system showed a faster response time when compared to a non-clustered system, indicating that parallel processing in a cloud-based environment is crucial for efficient template matching. C. Hahn et al. [14] stated that the primary cause of security vulnerabilities is inadequate randomness in the encryption of biometric databases. This weakness can manifest in the form of ciphertext-only attacks and known plaintext attacks, where the attacker can observe, access, or collude with cloud providers and users to obtain sensitive information. In addition, they also demonstrated that attackers can impersonate legitimate users and enter false information into the database, thereby obtaining a collection of plaintexts and their corresponding ciphertexts. To address these issues, a more randomized encryption method has been proposed to enhance the security of the database and identification queries in CloudBI. A security patch has been added to CloudBI. The suggested biometric authentication scheme has two stages. During the enrollment stage, a user extracts the fingerprint code from a fingerprint image and submits it to the DB owner. The DB owner then converts it into an (n + 2)-dimensional vector and matrix. This vector and matrix are later encrypted using two invertible matrices and a random lower triangular matrix with diagonal entries of 1. Finally, the encrypted data is sent to the cloud. During the identification process, DBowner extends and encrypts the finger code with a randomly selected value to prevent the enrollment of fake biometric data and the retrieval of an encrypted identification request. The similarity between two finger codes is calculated using matrix trace properties, which indirectly serve as a measure of Euclidean distance, resulting in accurate results. On average, CloudBI without a security patch is faster than the proposed scheme. However, the proposed security patch is effective against attackers at the enrollment level and is also practical. In [15], a new scheme is suggested primarily to reduce computational overload associated with the earlier privacy-preserving biometric identification schemes in the cloud. The authors from [16–19] discuss the framework, privacy-preserving techniques, and data security of cloud-based biometric traits. A method in [21] enhances template protection by utilizing NTRU homomorphic encryption and segregating the database and authentication server. It also includes an optimized decision-making strategy for identification and verification. The key components of the iris code are relocated to the beginning of the template to enable more efficient block-wise comparison, resulting in reduced comparison time. The iris code from the probe is rearranged and encrypted using the public key of the authentication server. The database calculates the encrypted total of the encrypted probe and reference after receiving the encoded probe and the subject's ID. The authentication server receives the sum and processes only one block at a time, decrypting it and determining the Hamming weight. Hamming weight is compared to two threshold values: δa (early accept border) and δr (early reject border). Each time a new block is evaluated, both criteria are adjusted whenever the hamming weight is between the two thresholds. In such a scenario, the following block is decrypted, and the previous value is incremented by the hamming weight. The database informs clients of whether the subject has been accepted or rejected. The authentication server determines the hamming distance between the initial block of the probe and the initial block of all references when in identification mode. A certain share is retained for future comparisons, while references with the highest Hamming distances are removed. Until all blocks have been analyzed or there is only one reference remaining, this procedure continues. The accuracy of identification decreases as the value of K (the share) decreases. Despite this, even in the worst scenario, an accuracy of 97% is still achieved, and it improves with higher values of K and security stages. The proposed design significantly reduces the number of block comparisons, leading to faster execution and overcoming the major challenges of homomorphic encryption schemes. However, it is important to note that increasing the security level will result in slower execution times for all transactions. Table 1 summarizes observations from several approaches.

Table 1. Summary of various approaches and their observations

Ref & Title of the Paper	Approach/Method	Observations
[1] Iris recognition based on Gabor and Deep Convolutional Networks	• Iris localization – circular Hough transform algorithm. • Normalization extracts the region of interest (ROI) • Iris enhancement • Feature extraction 1-D Gabor filter • CASIA dataset is considered	• Using the Gabor filter as a feature extractor and a neural network classifier, the model achieved 91.5% accuracy. • Using SVM as a classifier the model achieved 90% percent accuracy.
[2] Privacy preserving security using biometrics in cloud computing	• Face recognition-cloud security and privacy • Used double encryption and matching with stored data.	• Limitations -lower performance with small databases and slow matching process.
[3, 19, 21] Utilizing Transfer Learning and Homomorphic Encryption in a Privacy Preserving and Secure Biometric Recognition System	• Deep Zero ID method privacy-preserving biometric verification. • Homomorphic encryption to transform sensitive biometric • Utilizes transfer learning and Support Vector Machine.	• 95.47% F1 score in verifying combined iris and fingerprint features with no false positives.
[4] An Efficient Biometric Identification in Cloud Computing with Enhanced Privacy Security	• Orthogonal matrix property and randomness for privacy-preserving biometric identification	• Scheme requires less computational complexity and provides increased security, making it suitable for large databases.
[5] Efficient and Privacy-Preserving Online Fingerprint Authentication Scheme over Outsourced Data	• Online fingerprint authentication scheme called E-finga protects user privacy. enhanced homomorphic encryption system 2DNF	• Offers secure and reliable authentication without exposing the fingerprints
[6] A robust and secured cloud based distributed biometric system using symmetric key cryptography and Microsoft cognitive API	• Microsoft Cognitive face API used in cloud.	• Accuracy of 96% is achieved with 100 registered users face images and aadhar card images.
[7] An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing	• Encrypted finger codes used to withstand user and cloud collusion attacks. • Test finger code is extracted from a fingerprint image and compared with stored codes in cloud using Euclidean distance.	• Observed lesser preparation time and bandwidth consumption compared to other approaches and the same amount of time during identification.
[8] Multi-biometric Cryptosystem Based on Decision Level Fusion for File Uploading in Cloud	• Multimodal biometric cryptosystem was used or authentication. • Iris and fingerprint were used for login. LDA is applied to iris data for feature extraction. Binary iris features are extracted and transmitted to the server.	• Achieved 35 bits of security even with the attacker's knowledge of iris features • GAR was 15% with iris restrictions and 70% without iris restrictions.
[9] Artificial Neural Network Inducement for Enhancement of Cloud Computing Security	• AES encryption and an AI-based ANN for improved security. • User selects iris recognition or fingerprint recognition for biometric verification. Features are stored with Neural Network algorithms.	• AES's accuracy was found to be 94%.
[10, 20] Cancelable Biometrics Using Deep Learning as a Cloud Service	• System captures data, cross-folds it, embeds it in a QR code, and sends it to the cloud. • CNNs are used to extract features. • Cloud hosts a user authentication module using an MLP model.	• System achieved 80% accuracy on MMU data and 92% accuracy on FV-USM data. • Reduces processing time and cost compared to standalone biometric systems.

(Continued)

Table 1. Summary of various approaches and their observations *(Continued)*

Ref & Title of the Paper	Approach/Method	Observations
[11] A Model of A Biometric Recognition System Based On The Hough Transform of Libor Masek and 1-D Log-Gabor Filter	• High-quality iris images captured using high-resolution cameras • Hough Transform for segmentation • Gabor filters for feature extraction and Hamming distance for data matching.	• High accuracy rate, with 99.9236% overall accuracy on Casia V1 database and 99.4168% overall accuracy on MMU1 database. • Error rates (FAR, FRR, and EER) are low, but slightly higher on the MMU1 database.
[12, 16] Efficient and privacy-preserving biometric identification in cloud	• Symmetric homomorphic encryption for client's privacy.	• Scheme was developed using Java on Amazon EC2 cloud.
[13, 17, 18] An Efficient and Privacy-Preserving Biometric Identification Scheme Based on the FITing-Tree	• FITing tree and iDistance data structures were used to increase efficiency. • CS1and CS2, a client and the service provider servers were included in cloud	• Compared with MASK (considering synthetic dataset and Labeled Faces in the Wild (LFW) dataset) former has lesser running time providing a better accuracy.

3 PROPOSED SYSTEM

An iris-based authentication system is proposed to allow users to upload their iris images and verify their identity. The system processes uploaded images by performing pre-processing steps to enhance their quality and extract relevant features. These features are later encrypted using AES 128-bit encryption for secure transmission and storage. Encrypted feature vectors are stored in a cloud storage system that offers a scalable and secure storage infrastructure. Hamming distance helps in error detection and error correction during data transmission in computer networks. In coding theory, equal-length data words are compared. During authentication, the system retrieves encrypted feature vectors associated with the phone number and compares them with the features extracted from the test iris image using a Hamming distance calculation. The results of the matching process determine whether the user is authenticated or not, ensuring a reliable and secure authentication mechanism. Figure 1 depicts the system architecture of the proposed system.

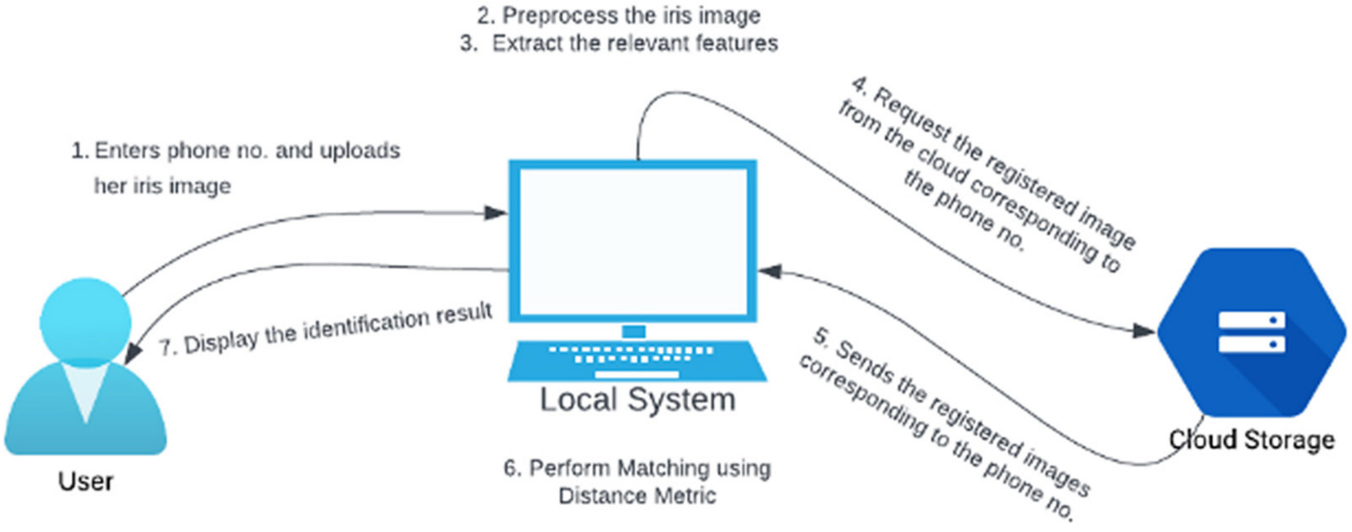

2. Preprocess the iris image
3. Extract the relevant features
1. Enters phone no. and uploads her iris image
4. Request the registered image from the cloud corresponding to the phone no.
7. Display the identification result
User
Local System
5. Sends the registered images corresponding to the phone no.
Cloud Storage
6. Perform Matching using Distance Metric

Fig. 1. System architecture

a) **Iris pre-processing.** Iris images are pre-processed to remove noise, enhance feature extraction, achieve localization accuracy, and reduce the computational load by working with smaller image sizes during iris localization. The proposed algorithm involves iris localization, normalization, and image enhancement to pre-process the image before feature extraction.

b) **Iris localization.** Localization benefits by capturing only the region of interest while discarding undesired sections. As a result, iris localization consistently plays a significant role in the preliminary processing phase, ensuring optimal efficiency. The proposed system utilizes the circular Hough transform algorithm to accomplish iris localization.

Localization is performed by implementing the following steps:

- Apply a bilateral filter to blur the image and reduce noise.
- The image coordinates are projected horizontally and vertically to find approximate center of the pupil based on the minimum values.
- Binarize a 120 × 120 region around the pupil using the estimated center to refine the estimation of the pupil center.
- Perform Canny edge detection on a masked image to extract edges around the pupil region.
- Utilize the Hough transformation to detect circles in the edge image, selecting the circle closest to the estimated pupil center as the pupil boundary.
- Draw the outer boundary by increasing the radius of the inner circle by 53.
- Store images with boundaries drawn in the “boundary” list and center coordinates in the “centers” list.

Iris normalization. Once the iris region has been precisely separated from an eye image, the subsequent task involves transforming the iris region into a standardized shape. Due to factors such as camera distance, illumination, and natural variations, the size of the iris may differ even within the same eye. To address this, a normalization process is employed to convert the iris region into consistent dimensions. The algorithm takes each image from the “boundary” list and creates an empty list to store normalized images. It focuses on the region between boundaries for projecting polar coordinates onto the Cartesian plane. Using a for loop with equally spaced intervals, the algorithm converts polar coordinates to Cartesian coordinates using the equations x = rcos(theta) and y = rsin(theta). Finally, the algorithm resizes the image to a rectangular size of 64 × 512.

Image enhancement. To address the challenges of low contrast and unclearness, it is necessary to employ techniques that enhance image quality. In this function, we employ histogram equalization to improve the image by enhancing its contrast. The process aims to increase the distinguishability of features within an image, enabling more effective feature extraction.

Feature extraction. A 1-D Gabor filter is used to extract various features from normalized iris images. Gabor filters are typically linear filters that detect edges and various features based on their spatial alignment. These filters are commonly used for analyzing textures and are a widely utilized technique for extracting features. Equations (1–3) indicate the formulas for calculating real, complex, and imaginary values.

$$\text{Complex } g(x, y, \lambda, \theta, \psi, \sigma, \Upsilon) = \exp(-(x'^2 + \Upsilon^2 y'^2)/2\sigma^2) \exp(I(2\pi(x'/\lambda) + \psi)) \tag{1}$$

$$\text{Real } g(x, y, \lambda, \theta, \psi, \sigma, \Upsilon) = \exp(-(x'^2 + \Upsilon^2 y'^2)/2\sigma^2) \cos(2\pi(x'/\lambda) + \psi) \tag{2}$$

$$\text{Imaginary } g(x, y, \lambda, \theta, \psi, \sigma, \Upsilon) = \exp(-(x'^2 + \Upsilon^2 y'^2)/2\sigma^2) \sin(2\pi(x'/\lambda) + \psi) \tag{3}$$

Where $x' = x\cos\theta + y\sin\theta$ and $y' = -x\sin\theta + y\cos\theta$

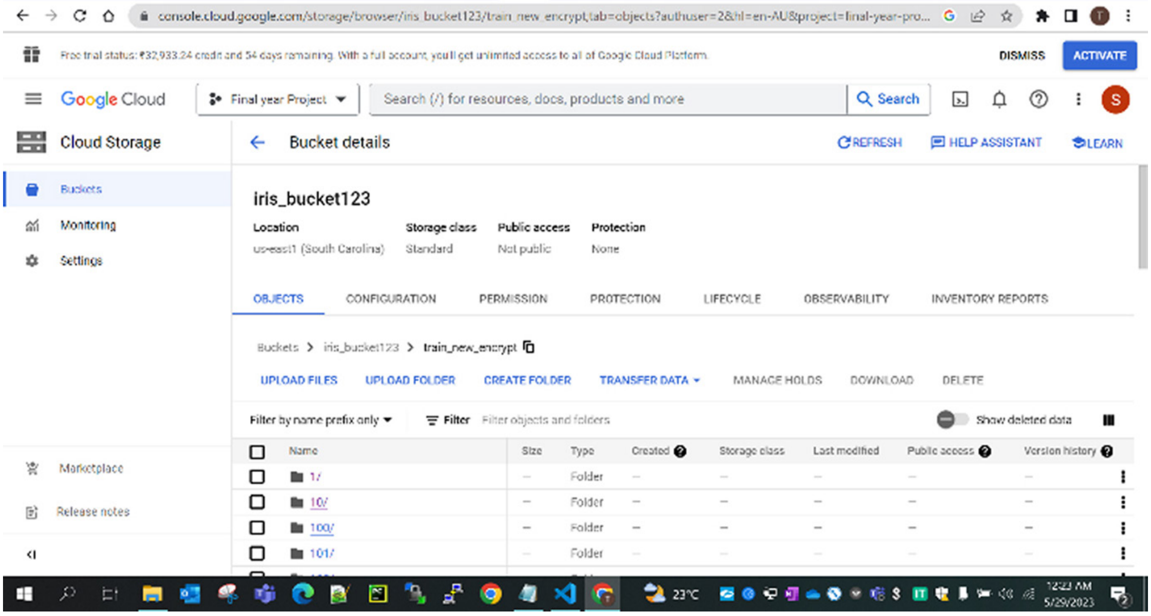
Equations represent a 2-D Gabor filter and are utilized on either the real or imaginary components, which are known as 1-D Gabor filters. Parameters in the equations have individual significance as they contribute to extracting distinct characteristics. Adjusting any of these parameters results in a new set of features. Hence, it is crucial to assign appropriate values to these parameters in order to achieve the desired characteristics. For our analysis, an 8×8 kernel size is applied in the Gabor filter. Subsequently, approximately 1536 attributes from an individual iris are collected and stored.

3.1 Retrieval from Google Cloud storage

Google Cloud provides computing resources for the development, deployment, and operation of web applications. Applications are built and maintained by GCP services. It monitors resource usage, such as data storage, network connectivity, processing power, and database queries. GCP software is leasedm and software can be developed based on a pay-as-you-go model.

Steps to retrieve the encrypted train folder from the cloud storage service of GCP corresponding to the user's phone number are as follows: Figure 2 depicts the GCP Cloud Storage console.

- The storage client is created.
- Check if the destination directory exists and create it if it does not.
- The bucket is retrieved from the storage client.
- Obtaining the list of blobs (files or directories) in a bucket with a specified prefix.
- Each blob is iterated over, and the following actions are performed:
  - The relative path of the blob is computed.
  - The destination file path is determined by combining the destination path and the relative path.
  - Necessary directories in the destination path are created if they do not exist.
  - The destination file path is opened in binary write mode.
  - The blob is downloaded and saved to the destination file.



console.cloud.google.com/storage/browser/iris_bucket123/train_new_encrypt;tab=objects?authuser=2&hl=en-AU&project=final-year-pro...

Free trial status: ₹32,933.24 credit and 54 days remaining. With a full account, you'll get unlimited access to all of Google Cloud Platform.

Bucket details

iris_bucket123

Location	Storage class	Public access	Protection
us-east1 (South Carolina)	Standard	Not public	None

Buckets > iris_bucket123 > train_new_encrypt

Filter by name prefix only ▾ Filter objects and folders

	Name	Size	Type	Created	Storage class	Last modified	Public access	Version history
□	1/	—	Folder	—	—	—	—	—
□	10/	—	Folder	—	—	—	—	—
□	100/	—	Folder	—	—	—	—	—
□	101/	—	Folder	—	—	—	—	—

Fig. 2. GCP cloud storage console

- If the download is successful, True is returned.
- If any exception occurs during the process, an error message is printed, and False is returned to indicate a download failure.

Iris matching. Hamming distance measures the dissimilarity between two iris codes by counting the number of differing bits. Iris images are converted into binary iris codes, which represent the patterns of the iris. By comparing the Hamming distances between an input iris code and iris codes retrieved from the cloud, a match or non-match decision is made by setting a threshold of 0.46. Euclidean and other distance metrics did not produce the expected output in multiple trials. Therefore, the Hamming distance was used to achieve the desired result. Equation 4 is used to calculate the Hamming distance.

hamming_dist = np. count_nonzero (np. array(list(iris1_bin))! = np. array (list(iris2_bin)))

$$\mathrm{DH} = \sum_{i=1}^{k} |x^{i} \quad y^{i}| \tag{4}$$

$$x = y \rightarrow D = 0$$
$$x \neq y \rightarrow D = 1$$

where, x and y are coordinates.

Advanced encryption standards secure data storage, transmission, and authentication, ensuring robust protection against potential threats and vulnerabilities. Attackers cannot gain unauthorized access to sensitive data because encryption is applied to iris feature vectors using AES. AES provides a high level of security with a 128-bit key and resistance against brute-force attacks. This guarantees the confidentiality and inaccessibility of encrypted feature vectors. AES encryption prevents collusion attempts between clients and the cloud to produce raw iris feature vectors. The encryption process makes it impossible for the cloud to retrieve actual feature vectors, ensuring data security and maintaining the confidentiality of sensitive information. Strong security features and proven reliability make the AES encryption algorithm a preferred choice. AES offers several key lengths, including 128-bit, 192-bit, and 256-bit. The 128-bit key scheme balances computational efficiency and security.

4 RESULTS

Accuracy. The accuracy of an iris recognition system can be measured in terms of true positives, true negatives, false positives, and false negatives. The proposed system achieved an accuracy of 92.39% by setting a threshold of 0.464615. This threshold was chosen to maximize true positives and true negatives while minimizing false positives and false negatives. There is a trade-off between accuracy and computational time. While our model may have slightly lower accuracy, it can still be considered computationally superior since it offers significantly faster processing times compared to other models.

Security analysis. A concise security analysis of the study is presented, focusing on the utilization of the AES as the encryption algorithm for secure data storage, transmission, and authentication. AES ensures robust protection against potential threats and vulnerabilities.

Attacker as a valid client. The possibility of an attacker impersonating a valid client and sending an identification request to the server and cloud is considered in the scheme. However, due to the encryption applied to iris feature vectors using AES, an attacker cannot gain unauthorized access to sensitive data. With a 128-bit key, AES provides a high level of security and resistance against brute-force attacks, ensuring the confidentiality and inaccessibility of encrypted feature vectors.

Collusion between the cloud and clients. AES encryption prevents collusion attempts between clouds and from harvesting raw iris feature vectors. The encryption process makes it impossible for the cloud to retrieve actual feature vectors, ensuring data security and maintaining the confidentiality of sensitive information.

AES as the optimal encryption algorithm. The selection of AES as the encryption algorithm is based on its strong security features and proven reliability. AES offers various key lengths, including 128-bit, 192-bit, and 256-bit. By choosing a 128-bit key, the scheme strikes a balance between security and computational efficiency. A 128-bit key size provides a robust level of security while minimizing computational overhead. Table 2 depicts the efficiency percentages of various algorithms.

Table 2. Percentage efficiency of various algorithms

Algorithms	Percentage Efficiency
DES	30
IDEA	60
Blow Fish	35
RSA	65
AES	90

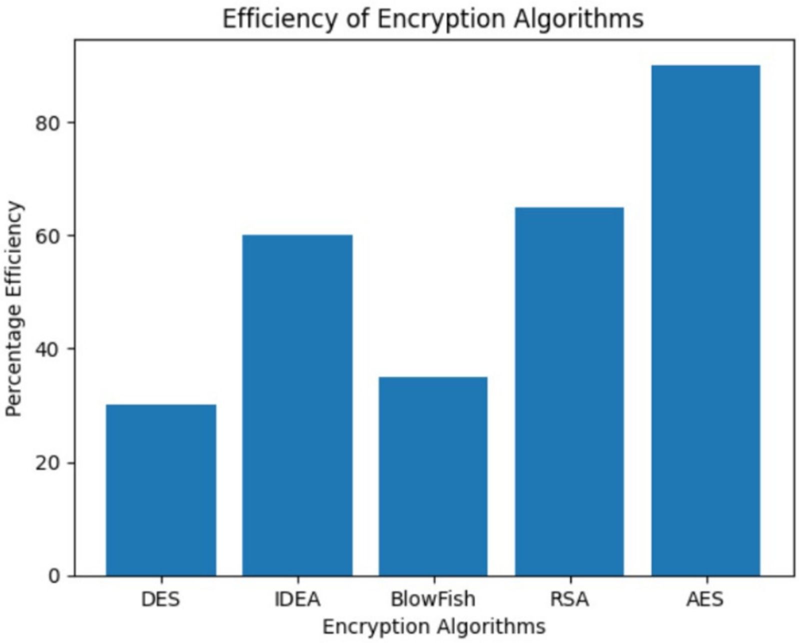


Fig. 3. Efficiency comparison of encryption algorithms

The inclusion of a graph in Figure 3 further solidifies the superiority of AES in terms of performance efficiency over other algorithms such as Rivest, Shamir, and Adleman (RSA), data encryption standards (DES), integrated development environment (IDE), and BLOWFISH. Visual representation serves as compelling evidence, reinforcing the resolute decision to select AES as the optimal encryption algorithm for the proposed scheme.

Time analysis. The estimated time it takes for a user's train folder to be downloaded from the cloud to their local system is determined. Below are the download times for all 108 folders.

download_train_folder_time = [7.635953187942505, 6.33191442489624, 6.248413324356079, 6.289820909500122, 7.560742378234863, 6.581365346908569, 6.256888389587402]

Average download time is found to be 6.91 seconds.

Figure 4 depicts a graph showing the time taken to download all the train folders of the 108 subjects. Figure 5 indicates a scatter plot of download time versus file size in KB.

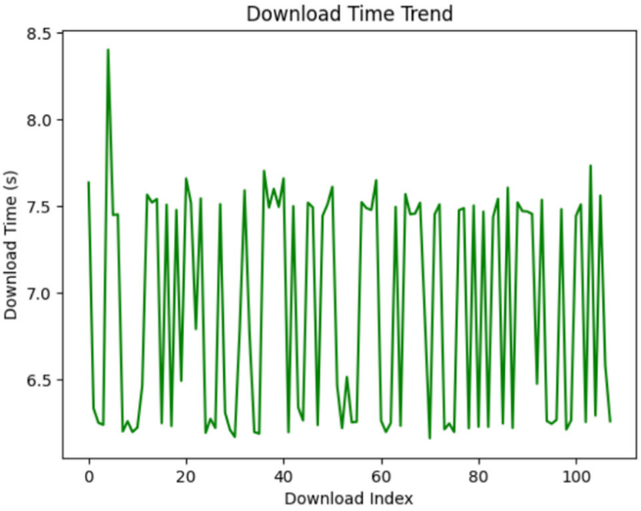


Fig. 4. Download time of traits

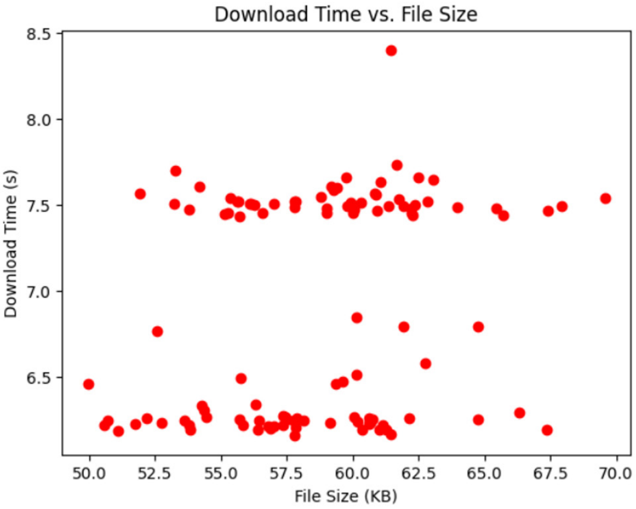


Fig. 5. Comparison of download time and file size

- The X-axis represents 108 subjects, while the Y-axis represents the time taken to download each of these subjects in seconds.
- The download time for most subjects varies between 6 to 7.5 seconds.
- Only a few outliers (5th subject) in the graph deviate from the general pattern observed.
  1. The X-axis represents the file sizes of all 108 subjects in kilobytes (KB), while the Y-axis represents the time taken to download each of these subjects in seconds.
  2. Download time for most subjects vary between 6 to 7.5 seconds.
  3. Very few subjects have a download time that falls within the range of 7 to 7.5 seconds.
  4. Most of the subjects' download time is either around 6 seconds or around 7.5 seconds.

Figure 6 represents a line graph indicating the time taken by the system to display identification results to the user.

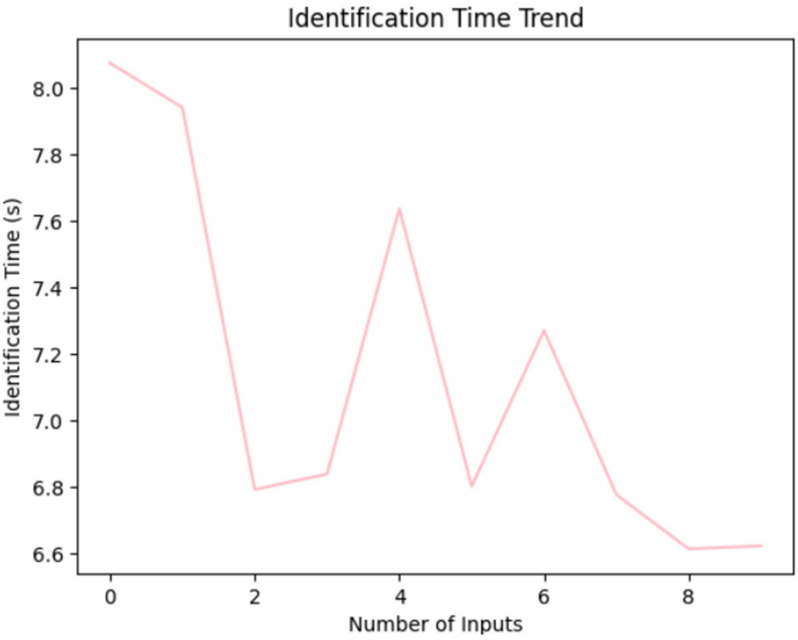
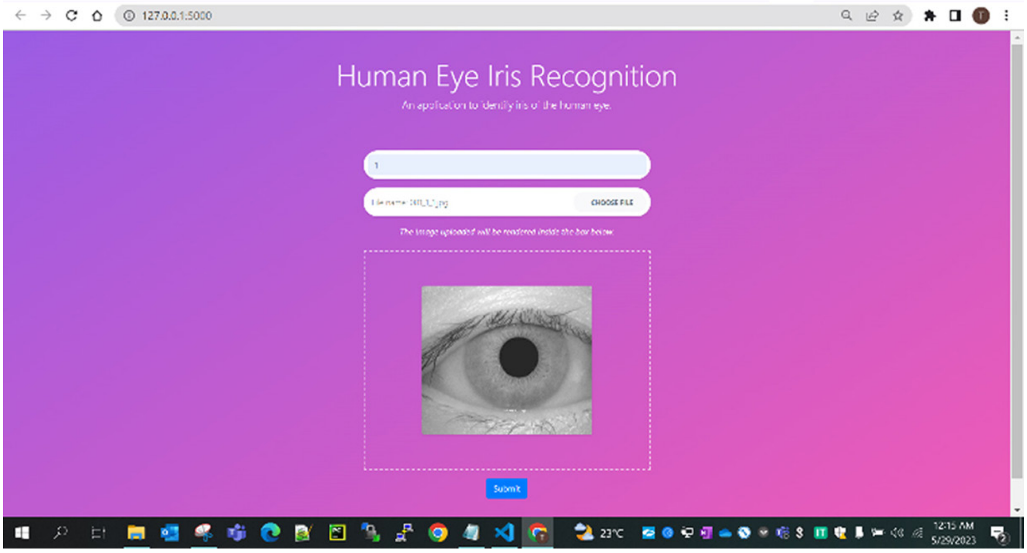


Fig. 6. Time taken for identification

- The X-axis represents 10 user inputs.
- The Y-axis represents the time taken by the system to identify the user's iris.
- The identification time ranges from 6.6 to 8.5 seconds.

4.1 GUI Snapshots

Figures 7 and 8 depict the GUI snapshots of human eye recognition system application and the detection of human eye recognition.


127.0.0.1:5000

Human Eye Iris Recognition

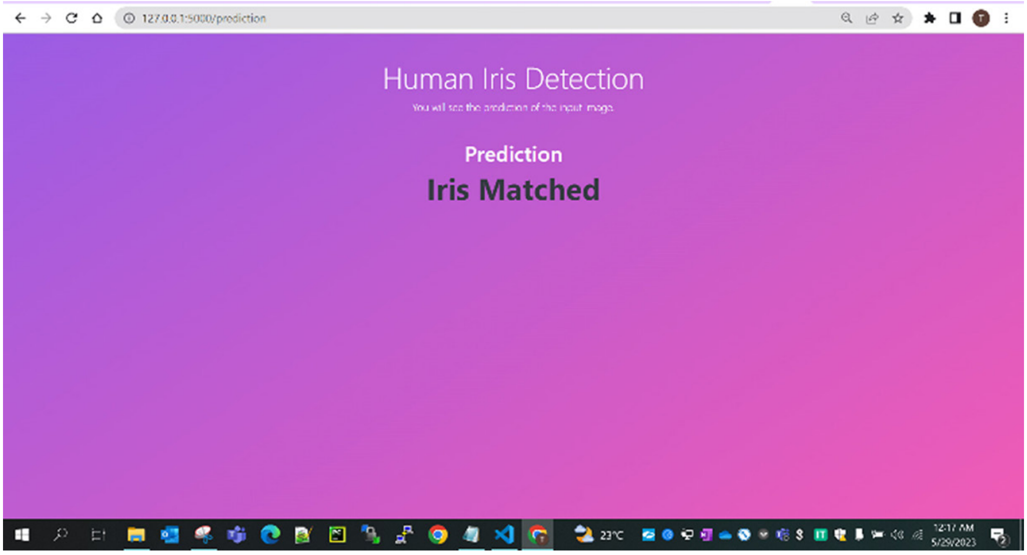
An application to identify iris of the human eye.

1

File name: [illegible]

The image uploaded will be rendered inside the box below.

Fig. 7. Snapshot of human eye recognition system



Human Iris Detection

You will see the prediction of the input image.

Prediction

Iris Matched

Fig. 8. Prediction application of iris matching

5 CONCLUSION

The proposed methodology prioritizes security and computational efficiency in iris-based authentication. Feature vectors of preprocessed data were stored to protect sensitive iris information. They were encrypted with AES 128-bit for added security during transmission and storage. Google Cloud Storage ensures scalable, reliable, and private storage. Computationally efficient pre-processing maintained accuracy for feature extraction, while the hamming distance calculation enabled fast and efficient matching of test and stored iris image features. The methodology established a secure and efficient authentication system that safeguards data and ensures reliable authentication results.

6 ACKNOWLEDGMENT

The authors would thank B.M.S. College of Engineering for supporting the research work.

7 REFERENCES

[1] S. Kumar, S. K. Singh, A. K., Singh *et al.*, "Privacy preserving security using biometrics in cloud computing," *Multimedia Tools Applications*, vol. 77, pp. 11017–11039, 2018. https://doi.org/10.1007/s11042-017-4966-5

[2] M. Salem, S. Taheri, and J. S. Yuan, "Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system," *Computers*, vol. 8, no. 1, p. 3, 2019. https://doi.org/10.3390/computers8010003

[3] C. Liu, X. Hu, Q. Zhang, J. Wei, and W. Liu, "An efficient biometric identification in cloud computing with enhanced privacy security," *IEEE Access*, vol. 7, pp. 105363–105375, 2019. https://doi.org/10.1109/ACCESS.2019.2931881

[4] H. Zhu, Q. Wei, X. Yang, R. Lu, and H. Li, "Efficient and privacy-preserving online fingerprint authentication scheme over outsourced data," *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 576–586, 2021. https://doi.org/10.1109/TCC.2018.2866405

[5] A. K. B. Halvi and S. Soma, "A robust and secured cloud based distributed biometric system using symmetric key cryptography and Microsoft cognitive API," in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, 2017, pp. 225–229. https://doi.org/10.1109/ICCMC.2017.8282681

[6] S. Preetha and S. V. Sheela, "New approach for multimodal biometric recognition," *Machine Learning for Predictive Analysis: Proceedings of ICTIS 2020*. Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-7106-0_45

[7] L. Zhu, C. Zhang, C. Xu, X. Liu and C. Huang, "An efficient and privacy-preserving biometric identification scheme in cloud computing," *IEEE Access*, vol. 6, pp. 19025–19033, 2018. https://doi.org/10.1109/ACCESS.2018.2819166

[8] V. S. Nair, G. N. Reshmypriya, M. M. Rubeena, and K. A. Fasila, "Multibiometric cryptosystem based on decision level fusion for file uploading in cloud," in *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*, 2017, pp. 29–32. https://doi.org/10.1109/ICRAECT.2017.19

[9] M. R. Uddin, K. M. Kabir, and M. T. Arefin, "Artificial neural network inducement for enhancement of cloud computing security," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019, pp. 1–6. https://doi.org/10.1109/ICASERT.2019.8934580

[10] S. Preetha and S. V. Sheela. "Multimodal biometric-based secured access mechanism for wireless sensor networks," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 9, pp. 86–99, 2022. https://doi.org/10.3991/ijoe.v18i09.30425

[11] T. Sudhakar and M. Gavrilova, "Cancelable biometrics using deep learning as a cloud service," *IEEE Access*, vol. 8, pp. 112932–112943, 2020. https://doi.org/10.1109/ACCESS.2020.3003869

[12] H. Djalal Rafik, S. Ahmed Mahmoudi, A. Reda, and M. Boubaker, "A model of a biometric recognition system based on the Hough Transform of Libor Masek and 1-D Log-Gabor filter," in *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, 2020, pp. 1–9. https://doi.org/10.1109/CloudTech49835.2020.9365917

[13] C. Hahn and J. Hur, "Efficient and privacy-preserving biometric identification in cloud," *ICT Express*, vol. 2, no. 3, pp. 135–139, 2016. https://doi.org/10.1016/j.icte.2016.08.006

[14] X. Yang, H. Zhu, S. Zhang, R. Lu, and X. Gao, "An efficient and privacy-preserving biometric identification scheme based on the FITing-tree," *Security and Communication Networks*, vol. 2021, 2021. https://doi.org/10.1155/2021/2313389

[15] K. R. Radhika and M. K. Nalini, "Biometric image encryption using DNA sequences and chaotic systems," in *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*, Bangalore, India, 2017, pp. 164–168. https://doi.org/10.1109/ICRAECT.2017.56

[16] P. Punithavathi, S. Geetha, and S. Shanmugam, "Cloud-based framework for cancelable biometric system," in *2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2017, pp. 35–38. https://doi.org/10.1109/CCEM.2017.13

[17] C. Hahn, H. Shin, and J. Hur, "Cloud-based biometrics processing for privacy-preserving identification," in *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2017, pp. 595–600. https://doi.org/10.1109/ICUFN.2017.7993859

[18] J. Kolberg, P. Bauspieß, M. Gomez-Barrero, C. Rathgeb, M. Dürmuth, and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2019, pp. 1–6. https://doi.org/10.1109/WIFS47025.2019.9034982

[19] M. K. Nalini and K. R. Radhika, "Angular similarity based cancelable biometrics authentication for remote/cloud applications," in *AIP Conference Proceedings*, 2022. https://doi.org/10.1063/5.0109727

[20] J. Kolberg, P. Bauspieß, M. Gomez-Barrero, C. Rathgeb, M. Dürmuth, and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2019, pp. 1–6. https://doi.org/10.1109/WIFS47025.2019.9034982

[21] A. A. Al-Janabi, S. T. F. Al-Janabi, and B. Al-Khateeb, "Secure data computation using deep learning and homomorphic encryption: A survey," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 11, pp. 53–82, 2023. https://doi.org/10.3991/ijoe.v19i11.40267

8 AUTHORS

Dr. Nalini M K holds a PhD in Biometric Encryption from Visvesvaraya Technological University, India. She is currently working as an Assistant Professor at the Department of Information Science & Engineering at B.M.S. College of Engineering. Her research interest are Biometrics, Cryptography Network Security. She has several publications to her credit. She can be contacted at E-mail: nalini.ise@bmsce.ac.in; ORCID: https://orcid.org/0000-0003-3817-0593.

Preetha S received Bachelor's degree in Computer Science & Engineering from Visvesvaraya Technological, India, in 2007 and M. Tech degree in Computer Network Engineering in 2011. Currently, she is an Assistant Professor at the Department of Information Science & Engineering, B.M.S. College of Engineering. Her research interests include biometric Authentication, Social Area Networking, Wireless Sensor Networks, She can be contacted at E-mail: preetha.ise@bmsce.ac.in; ORCID: https://orcid.org/0000-0003-4160-8656

Sumedha Samanta, Tejaswini V, and Yashasvi M are students of Information Science & Engineering from B.M.S. College of Engineering. They can be contacted at E-mail: sumedha.is19@bmsce.ac.in, tejaswiniv.is19@bmsce.ac.in, yashasvim.is19@bmsce.ac.in