🌐 *United International Journal of Engineering and Sciences* 🌐
(UIJES – A Peer-Reviewed Journal); ISSN:2582-5887 | Impact Factor:8.075(SJIF)
Volume 5 | Special Issue 1 | 2025 Edition
National Level Conference on "Advanced Trends in Engineering Science & Technology" – Organized by RKCE

Secure Cloud Access Using Cryptographic and Biometric Authentication

Garapati Mary[1,a)],Shaik Mahabu Subani[2,b)], M Anvesh[3,c)]

[1]Asst. Professor, Department of Master of Computer Applications,Tirumala Institute of Technology and Sciences ,Satuluru-522601, Narasaraopet, Andhra Pradesh, India
[2]MCA student, Department of Master of Computer Applications, Tirumala Institute of Technology and Sciences ,Satuluru-522601, Narasaraopet, Andhra Pradesh, India
[3]Asst. Professor, Department of Mechanical Engineering, R K College of Engineering, Vijayawada-521456, Andhra Pradesh, India

*Correspondence E-mail: [a)]marygarapati12@gmail.com
[b)]sksubani367@gmail.com
[c)]anvesh.malneedi8@gmail.com

***Abstract*-TCloud computing has achieved maturity, and there is a heterogeneous group of providers and cloud- based services. However, significant attention remains focused on security concerns. In many cases, security and privacy issues are a significant barrier to user acceptance of cloud computing systems and the advantages these offer with respect to previous systems. Biometric technologies are becoming the key aspect of a wide range of secure identification and personal verification solutions, but in a cloud computing environment they present some problems related to the management of biometric data, due to privacy regulations and the need to trust cloud providers. To overcome those problems in this paper, we propose a crypto biometric system applied to cloud computing in which no private biometric data are exposed**

***Keywords*- Biometric Authentication, Cloud Security,Secure Framework, Cloud Environments, Privacy Protection, Identity Verification, Authentication Protocols, Data Encryption.**

I.INTRODUCTION

As cloud computing continues to evolve, the need for robust security mechanisms to protect sensitive data and ensure secure access has become increasingly important. Cloud environments are vulnerable to a wide range of security threats, including unauthorized access, data breaches, and identity theft. To address these concerns, traditional authentication methods, such as passwords and PINs, are proving to be insufficient due to their vulnerability to attacks like phishing, brute force, and credential theft. This has led to a growing demand for more secure and advanced authentication techniques

Cryptographic and biometric authentication are two promising technologies that offer a higher level of security compared to conventional methods. Cryptography ensures the confidentiality and integrity of data by encrypting sensitive information, while biometrics, which include fingerprint recognition, facial recognition, and iris scanning, offer a unique and hard-to-replicate form of user identification

By combining these two approaches, a more robust and resilient authentication system can be developed, capable of providing both strong user verification and protection against various cyber threats. This paper explores the integration of cryptographic techniques with biometric authentication in the context of cloud computing. The aim is to enhance the security of cloud access by leveraging the strengths of both technologies, creating a multi-layered authentication system that is more resistant to unauthorized access and data breaches

Through this integrated approach, we aim to provide a comprehensive solution that ensures secure and seamless user authentication while maintaining the privacy and integrity of cloud-based systems. This paper will delve into the various cryptographic algorithms and biometric modalities that can be applied to cloud security, discussing their benefits, challenges, and the potential they offer for securing cloud environments.

II. LITERATURE SURVEY

Biometric authentication has become a cornerstone for secure user identification, relying on unique physical and behavioral characteristics such as fingerprints, facial features, voice patterns, and iris scans. Among these, fingerprint recognition has long been the most widely adopted biometric method due to its simplicity, accuracy, and relatively low cost of implementation. However, with advancements in technology, facial recognition has emerged as a highly effective and user-friendly alternative, particularly with the integration of deep learning algorithms that have improved its accuracy and robustness against environmental factors like lighting and facial angle. Iris recognition offers even higher security levels due to the uniqueness of the iris and its stability over time, making it one of the most secure biometric modalities. Despite these strengths, all biometric systems face challenges, such as spoofing attacks (where fake biometric traits can be used to bypass authentication), environmental variability (such as changes in lighting conditions or user positioning), and the need for robust matching algorithms that can handle large datasets efficiently without compromising accuracy. Research continues to focus on improving the resilience of biometric systems against such challenges, enhancing their security and user experience.

The integration of biometric authentication into cloud environments presents a range of complex challenges, particularly concerning privacy, security, and data management. Cloud computing offers immense flexibility and scalability for storing and processing large amounts of data, including biometric information, but it also raises concerns about the safety and confidentiality of such sensitive data. One of the critical issues is the storage and transmission of biometric data, as it must be safeguarded against potential cyberattacks and unauthorized access. As a result, several security protocols have been proposed to protect biometric data in cloud environments, such as end-to-end encryption which aim to secure the biometric information both in transit and while stored. Additionally, secure multi-party computation (SMC) has been explored to enable computation on encrypted biometric data without exposing it to unauthorized entities. Another significant challenge is ensuring the scalability of biometric authentication systems in cloud infrastructures, as real-time processing of biometric data for thousands or even millions of users can lead to delays and performance bottlenecks. Research has been focused on reducing latency and ensuring high throughput in cloud-based biometric systems, but the trade-off between high performance and security Recent advances in security frameworks for cloud-based biometric systems have introduced several innovative technologies to further enhance privacy and security. One of the most promising solutions is the use of blockchain technology**,** which provides a decentralized and immutable ledger for recording biometric data and authentication transactions. This ensures data integrity and offers a transparent audit trail that can be crucial for maintaining trust and accountability in cloud systems. Another breakthrough is homomorphic encryption, a technique that allows biometric data to be processed while it remains encrypted, thus preventing exposure during computation. This makes it possible to perform secure biometric authentication in the cloud without revealing sensitive information to external parties. Federated learning**,** an emerging approach in machine learning, is also gaining attention. It enables decentralized model training**,** where biometric data is kept on users' devices and only model updates are sent to the central server, preventing the central storage of sensitive biometric data. These frameworks not only offer enhanced security and privacy but also address the scalability issues of cloud-based biometric systems. Looking to the future, AI-powered biometric **systems** will continue to evolve, improving the accuracy and efficiency of biometric recognition while leveraging advanced cryptographic methods to address ongoing privacy and security concerns in cloud environments.

III. **P**ROPOSED **M**ETHODOLOGY

The proposed methodology combines cryptographic techniques and biometric authentication to ensure a secure and efficient cloud access system. This multi-layered authentication system strengthens security by incorporating both encryption and user identification through biometric traits. The system design includes the following component

1. System Overview The architecture includes the following key components:

- User Device: The device used by the user (e.g., smartphone, laptop) for accessing the cloud. It contains biometric sensors and cryptographic modules.
- Authentication Server: The cloud server that processes authentication requests, verifying the user's credentials with both cryptographic and biometric methods.
- Biometric Database: A secure database where encrypted biometric templates (e.g., fingerprints, facial data) are stored.
- Cryptographic Module: The cryptographic system for encrypting and securing data storage and communication between the user device and the cloud server.
- Communication Layer: Ensures secure data transmission between the user device and cloud using encryption protocols like TLS/SSL

Technology Used

1. Cryptographic Technologies:

- Public Key Infrastructure (PKI): Secure communication using public and private keys.
- AES (Advanced Encryption Standard): Symmetric encryption for securing data.

- RSA: Asymmetric encryption for secure communication.
- TLS/SSL: Protocols for secure data transmission between user and cloud.
- Digital Signatures: Verify authenticity and integrity of data.

2 Biometric Authentication:

- Fingerprint Recognition: Authenticating users based on fingerprint data.
- Facial Recognition: Using facial features for identification.
- Voice Recognition: Identifying users by voice patterns.
- Liveness Detection: Ensures biometric data comes from a live person

3 **Multi-Factor Authentication (MFA)**:

- PIN/Password: Traditional authentication factor.
- OTP (One-Time Password): Additional authentication layer.

4 **Cloud Security**:

- Cloud Storage Security: Ensures encrypted storage of user data.
- Blockchain: Decentralized biometric data storage for added security.

5 **Secure Communication**:

- OAuth/JWT: Secure token-based authentication for access control.

6 **Anti-Spoofing**:

- Liveness Detection: Prevents spoofing by verifying the liveliness of biometric data.
- Deep Learning for Facial Recognition: Enhances accuracy and anti-spoofing capabilities.

IV. **S**YSTEM **A**RCHITECTURE

A cryptographic biometric authentication solution for cloud computing addresses key security and privacy concerns by encrypting biometric data at every stage—from capture to storage and processing. It ensures that sensitive data, such as fingerprints or facial features, is securely transformed into encrypted templates that cannot be easily reconstructed or tampered with. The authentication process compares encrypted templates using homomorphic encryption, maintaining privacy during verification. The system also leverages blockchain technology to provide an immutable and auditable record of authentication events, adding transparency and preventing fraud. With scalability, the solution supports large volumes of data while meeting regulatory compliance (e.g., GDPR, HIPAA) through secure data handling practices. Additionally, key management protocols ensure that encryption keys are securely managed, rotated, and revoked to protect access to biometric data, making this approach highly secure and adaptable for cloud-based services.

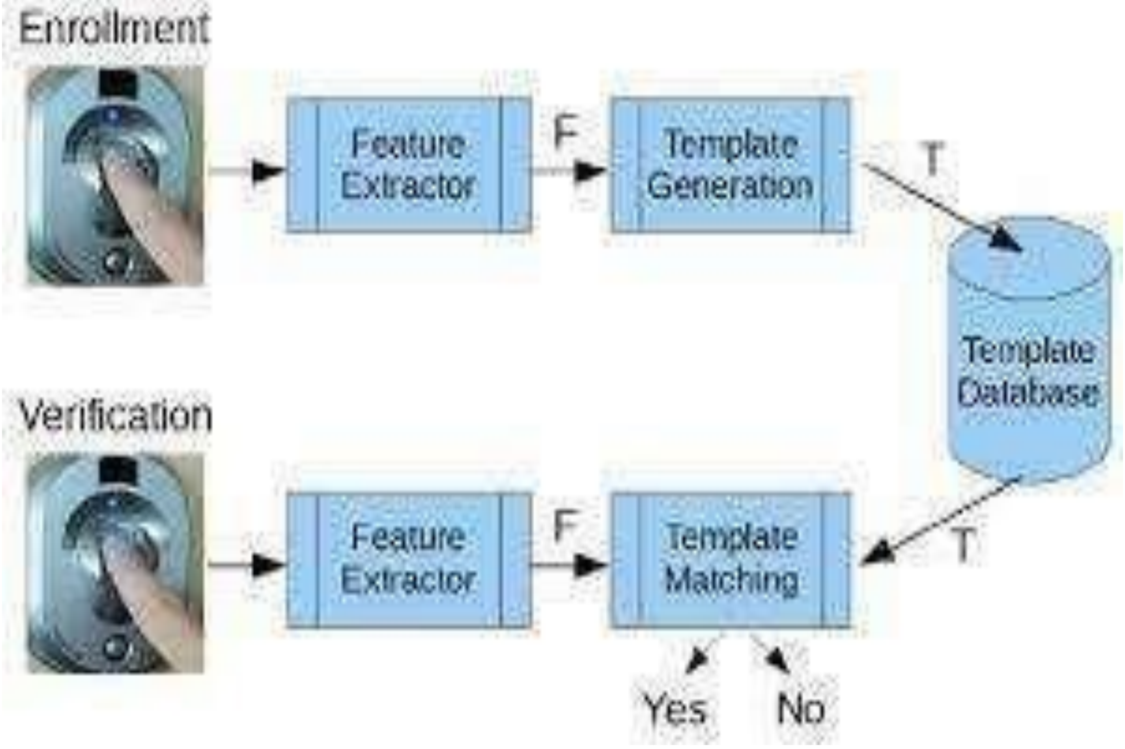


Figure 1: System Architecture

MODULES:

1) Upload Fish Dataset: using this module we will upload dataset to application
2) Run Interpolation, CLAHE & LAB: using this module we will read all images and then apply interpolation, CLAHE and LAB to process all images and then normalize images and then split dataset into train and test
3) Run Decision Tree: processed train images will be input to decision tree to trained a model and this model will be applied on TEST images to calculate prediction accuracy and other metrics
4) Run Logistic Regression: processed train images will be input to logistic regression to trained a model and this model will be applied on TEST images to calculate prediction accuracy and other metrics
5) Run Naive Bayes: processed train images will be input to naïve bayes to trained a model and this model will be applied on TEST images to calculate prediction accuracy and other metrics
6) Run Propose SVM Algorithm: processed train images will be input to SVM algorithm to trained a model and this model will be applied on TEST images to calculate prediction accuracy and other metrics
7) Comparison Graph: using this module we will plot accuracy and other metric graphs
8) Predict Fish Status: using this module we will upload test image and then SVM algorithm will predict whether image contains fresh or infected fish

V. METHODOLOGY

1. **User Enrollment Process**:

- Biometric Data Capture**:** The user's biometric data (fingerprint, face scan, or voice pattern) is captured using sensors on the user's device.
- Biometric Template Creation**:** The captured data is processed into a digital template (e.g., a mathematical representation of the fingerprint or facial features).
- Encryption and Storage: The biometric template is encrypted using a cryptography

2. Authentication Process:

- User Device Authentication**:** The user initiates access by providing biometric data (e.g., fingerprint scan or facial recognition) and/or cryptographic credentials (e.g., PIN or password).
- Biometric Verification**:** The captured biometric data is encrypted and compared with the stored biometric template in the cloud. If it matches, the system proceeds to the next step.
- Cryptographic Authentication**:** The user's cryptographic credentials (PIN, password) are verified on the server using encryption methods like RSA or AES.
- Multi-Factor Authentication**:** Both the biometric data and cryptographic credentials must be validated before granting access to the cloud resources

3. Secure Data Communication:

- TLS/SSL Encryption**:** After successful authentication, the communication between the user device and the cloud server is secured using TLS/SSL protocols, ensuring that all data exchanged is encrypted.
- Session Token Generation: Once authenticated, a secure session token (via OAuth **or** JWT**)** is generated to maintain the user's access to cloud resources without needing to authenticate repeatedly.

4. Anti-Spoofing and Liveness Detection:

- Liveness Detection**:** The system incorporates liveness detection to ensure that the biometric data provided is from a live user and not a replica (e.g., photo or video). This prevents spoofing attacks.
- Deep Learning for Facial Recognition**:** Advanced algorithms (such as deep learning) are used to enhance the accuracy of facial recognition systems and improve resistance to spoofing

5. Data Security and Privacy:

- Encryption of Biometric Data**:** All biometric data is encrypted during storage and transmission to ensure privacy and prevent unauthorized access.
- Blockchain for Decentralized Storage**:** Biometric templates may be stored in a decentralized manner using blockchain or distributed ledger technology, ensuring data integrity and reducing centralized data risks.

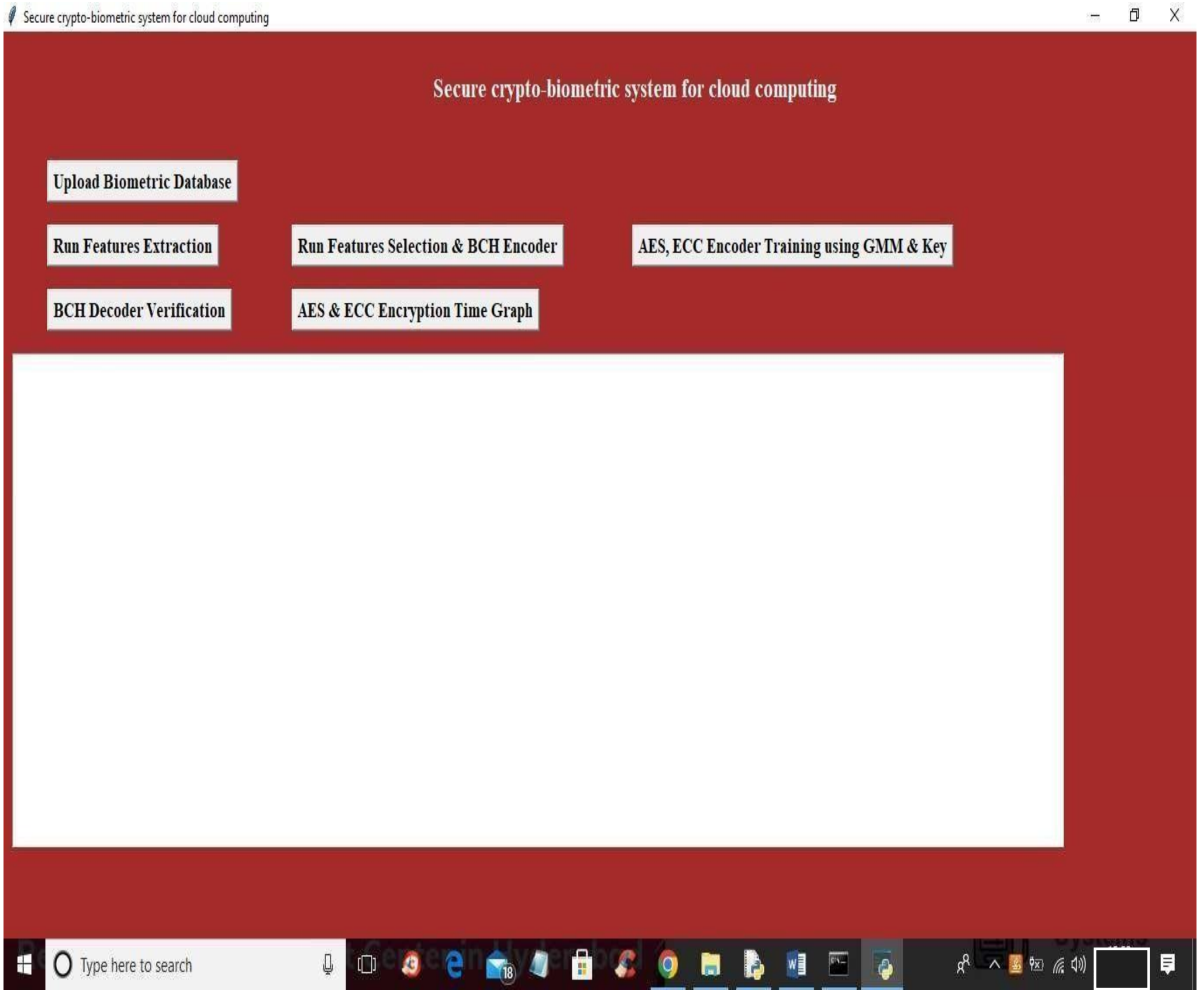
6. Session Management:

- Secure Session Tokens**:** After successful authentication, the user is assigned a JWT (JSON Web Token) **or** OAuth token that enables secure, token-based session management. This ensures that the user does not need to authenticate repeatedly during the session.

Summary of the Methodology:

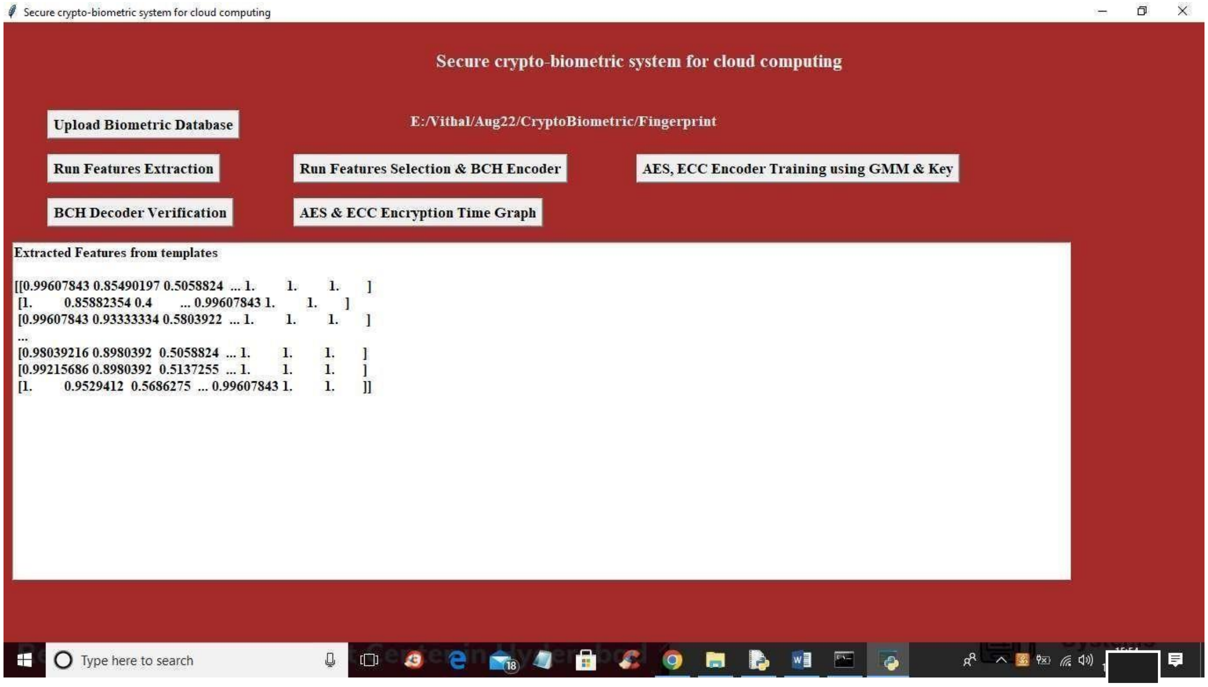
- Biometric Enrollment and Storage**:** Capture, process, encrypt, and store biometric templates.
- Multi-Factor Authentication**:** Use both biometric data and cryptographic credentials (PIN/password) for access.
- Secure Communication**:** Encrypt data transmission using TLS/SSL and use session tokens.

RESULT

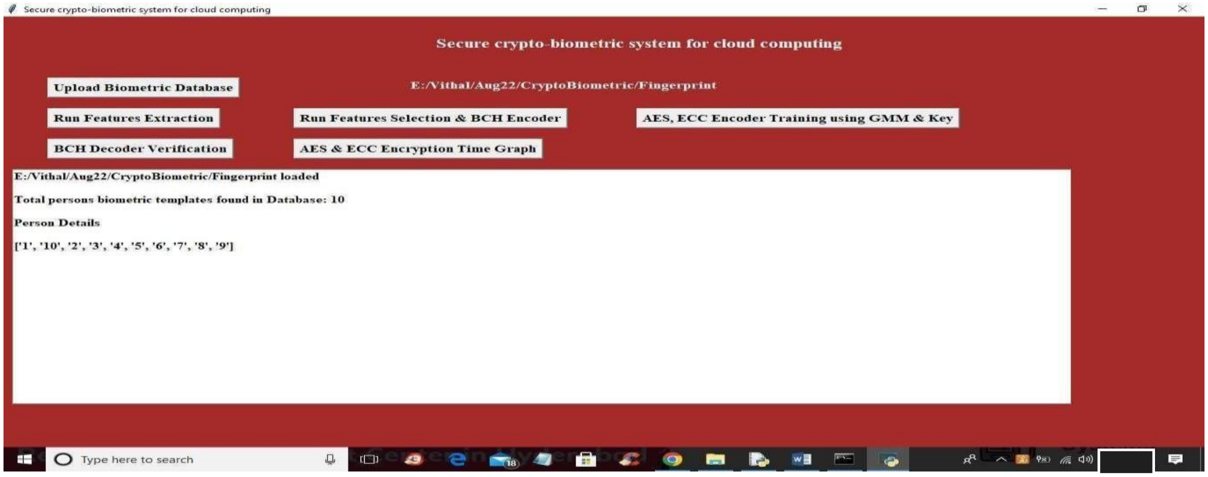

Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Type here to search

To run project double click on _run.bat‘ file to get below screen

In above screen click on _Upload Biometric Database‘ button to upload biometric data and get below output   In above screen selecting and uploading Finger biometric images dataset and then click on _Select Folder‘ button to load database and get below output

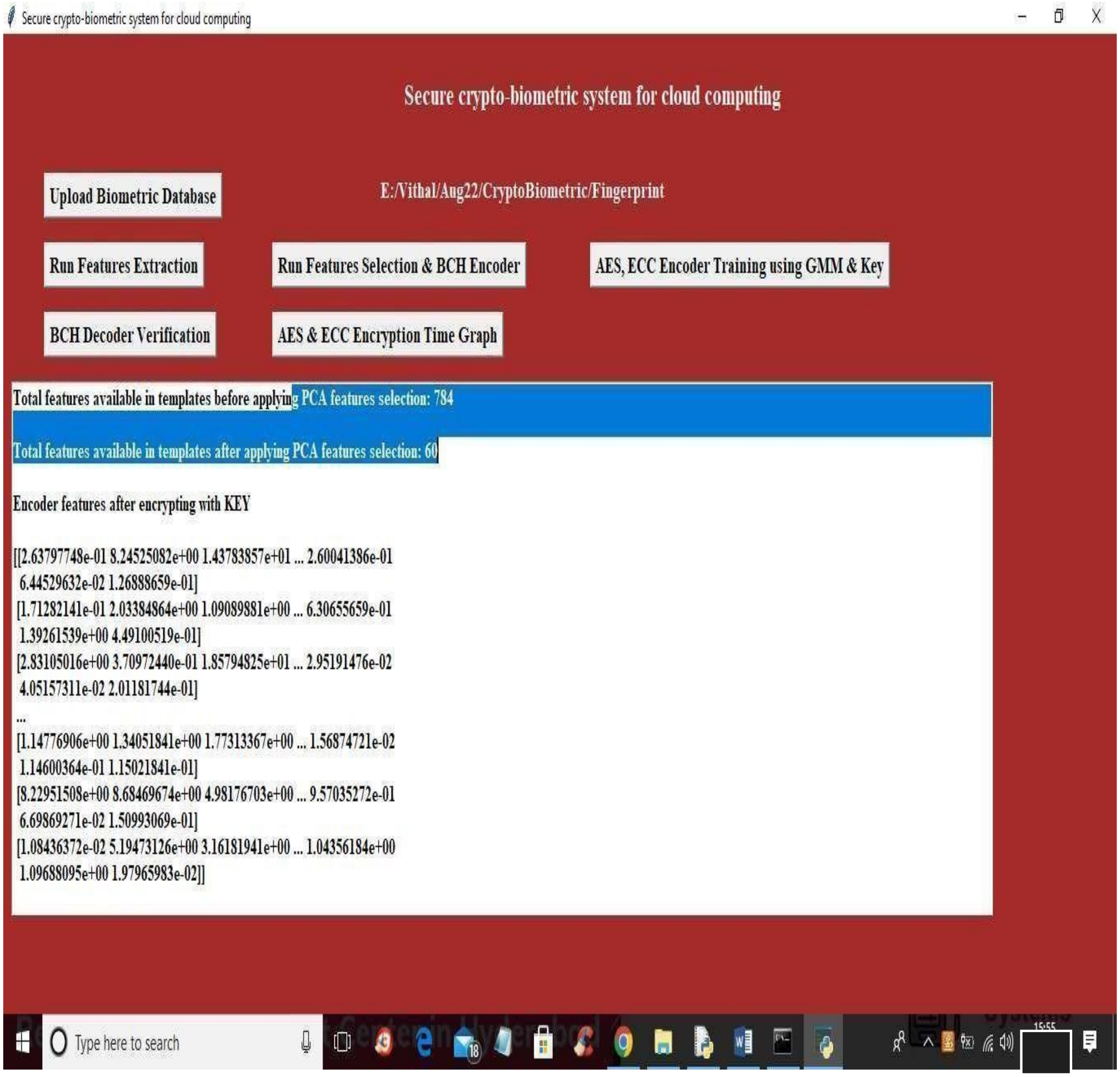

Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
E:/Vithal/Aug22/CryptoBiometric/Fingerprint
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Type here to search

```
Extracted Features from templates

[[0.99607843 0.85490197 0.5058824  ... 1.         1.         1.        ]
 [1.         0.85882354 0.4        ... 0.99607843 1.         1.        ]
 [0.99607843 0.93333334 0.5803922  ... 1.         1.         1.        ]
 ...
 [0.98039216 0.8980392  0.5058824  ... 1.         1.         1.        ]
 [0.99215686 0.8980392  0.5137255  ... 1.         1.         1.        ]
 [1.         0.9529412  0.5686275  ... 0.99607843 1.         1.        ]]
```


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
E:/Vithal/Aug22/CryptoBiometric/Fingerprint
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Type here to search

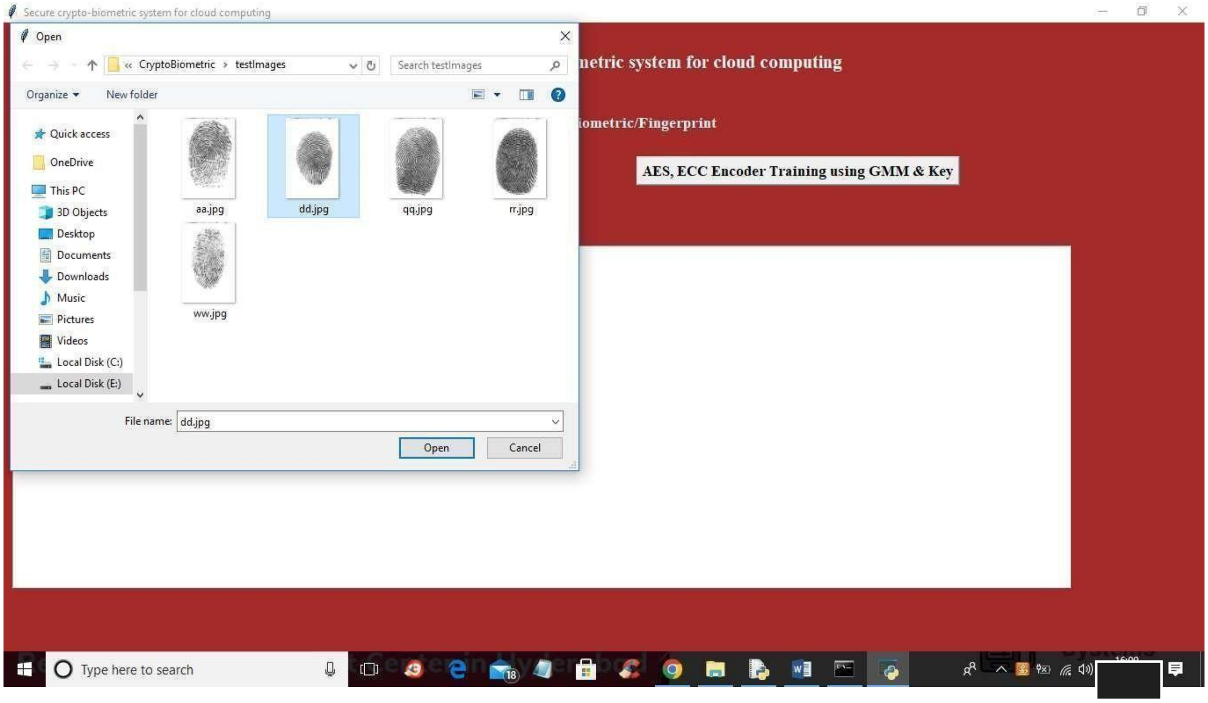
```
E:/Vithal/Aug22/CryptoBiometric/Fingerprint loaded

Total persons biometric templates found in Database: 10

Person Details

['1', '10', '2', '3', '4', '5', '6', '7', '8', '9']
```

In above screen we can see database loaded and we can see it contains biometric template of 10 different persons and now click on _Run Features Extraction‘ button o extract features from templates and get below output


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
E:/Vithal/Aug22/CryptoBiometric/Fingerprint
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Type here to search

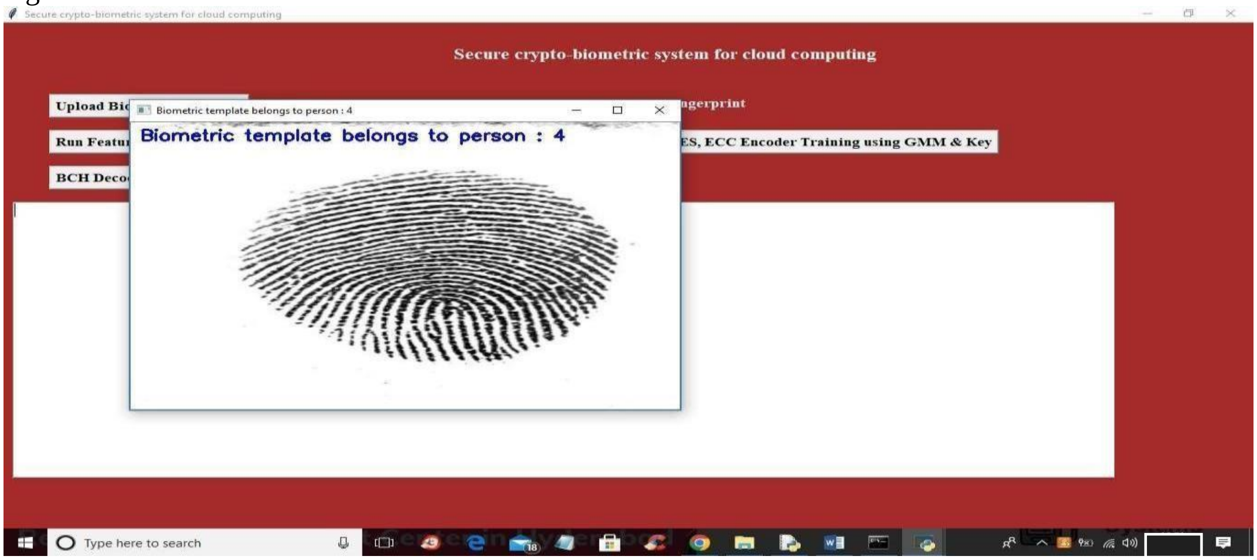
```
Total features available in templates before applying PCA features selection: 784

Total features available in templates after applying PCA features selection: 60

Encoder features after encrypting with KEY

[[2.63797748e-01 8.24525082e+00 1.43783857e+01 ... 2.60041386e-01
  6.44529632e-02 1.26888659e-01]
 [1.71282141e-01 2.03384864e+00 1.09089881e+00 ... 6.30655659e-01
  1.39261539e+00 4.49100519e-01]
 [2.83105016e+00 3.70972440e-01 1.85794825e+01 ... 2.95191476e-02
  4.05157311e-02 2.01181744e-01]
 ...
 [1.14776906e+00 1.34051841e+00 1.77313367e+00 ... 1.56874721e-02
  1.14600364e-01 1.15021841e-01]
 [8.22951508e+00 8.68469674e+00 4.98176703e+00 ... 9.57035272e-01
  6.69869271e-02 1.50993069e-01]
 [1.08436372e-02 5.19473126e+00 3.16181941e+00 ... 1.04356184e+00
  1.09688095e+00 1.97965983e-02]]
```

In above screen features extracted and now click on _Run Features Selection & BCH Encoder‘ button to select features from extracted features



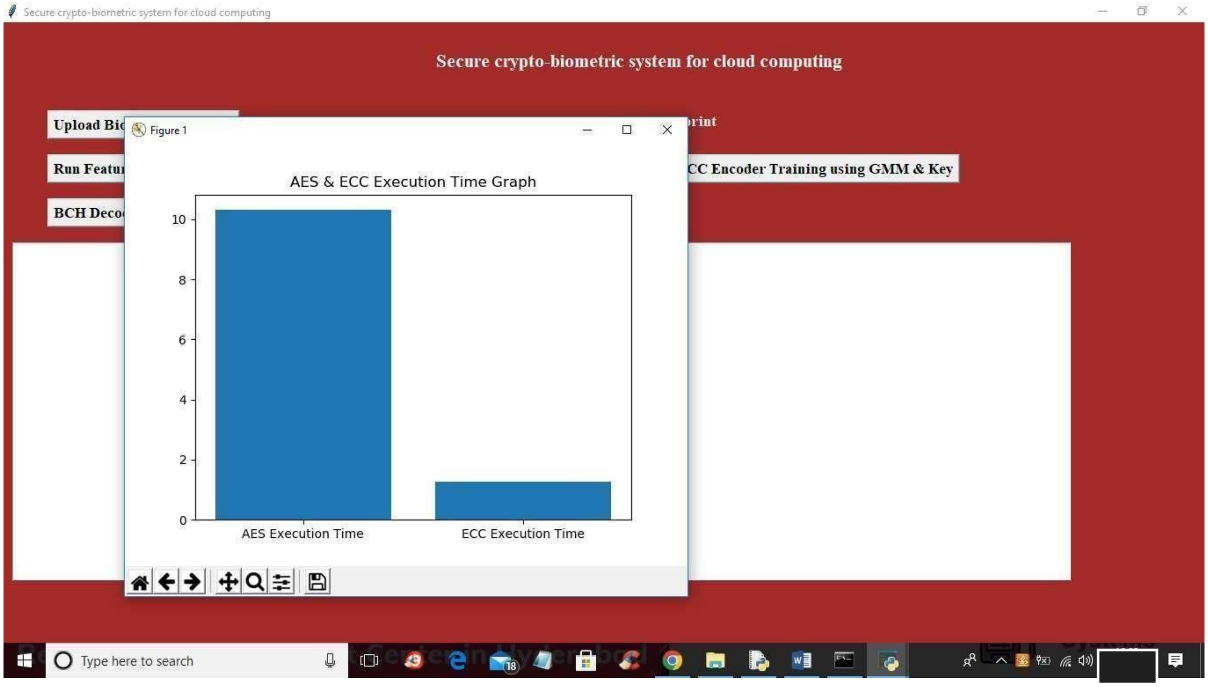
File name: dd.jpg

In above screen before applying PCA features selection algorithm, we have 784 features and then PCA select 60 important features out of it and now click on _AES, ECC Encoder Training using GMM & Key‘ button to encode features and then train GMM and this GMM will get encrypted using ECC and AES algorithms



Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Bio
Run Featu
BCH Deco
ngerprint
ES, ECC Encoder Training using GMM & Key
Biometric template belongs to person : 4
Type here to search

Biometric template belongs to person : 4


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Bio
Run Featur
BCH Deco
rint
CC Encoder Training using GMM & Key
Figure 1
AES & ECC Execution Time Graph
0
2
4
6
8
10
AES Execution Time
ECC Execution Time
Type here to search

and then will get below output

CONCLUSION

We introduce a significant machine learning-based classification model (SVM) to identify infected fishes in this research work. The real-world without augmented dataset (163 infected and 68 fresh) and augmented dataset (785 infected and 320 fresh) are used to train our model is new and novel. We mainly classify fishes into two individual classes: fresh fish and another is infected fish. We appraise our model with various metrics and show the classified outcome with visual interaction from those classification results. Besides developing our classifier, it means segmentation, cubic spline interpolation, and adaptive histogram equalization for transforming our input image more adaptable to our classifier. We also compare our model results with three classification models and observe that our proposed classifier is the best solution in this case.

This work contributes to bringing out a superior automated fish detection system than the existed systems based on image processing or lower accuracy. We not only depend on the modern image processing technique but also adjoin demandable supervised learning techniques. We prosperously develop the classifier that predicts infected fish with the best accuracy rate than other systems for our real-world novel dataset.

In the future, we stratagem to utilize various Convolutional Neural Networks (CNN) architecture for identifying fish disease more precisely and meticulously. Moreover, we will focus on the implementation of a real-life IoT device using the proposed system. Doing so can be a specific solution for the farmers in aquaculture to identify infected salmon fishes and take proper steps before facing any unexpected loss in their farming. We willwork with different fish datasets to make our system more usable in other sectors of aquaculture. We will also concentrate on increasing our existing dataset as salmon fish is one of the demanding elements worldwide.

REFERENCES

[1] A. A. M. Abd Hamid, N. and A. Izani. Extended cubic b-spline interpolation method applied to linear two- point boundary value problem. World Academy of Science, 62, 2010.

[2] T. Acharya. Median computation-based integrated color interpolation and color space conversion methodology from 8-bit bayer pattern rgb color space to 24-bit cie xyz color space, 2002. US Patent 6,366,692.

[3] A. F. Agarap. An architecture combining convolutional neural network (cnn) and support vector machine (svm) for image classification. arXiv preprint arXiv:1712.03541, 2017.

[4] A. Ben-Hur and J. Weston. A user‘s guide to support vector machines. In Data mining techniques for the life sciences, pages 223– 239. Springer, 2010.

[5] S. Bianco, F. Gasparini, A. Russo, and R. Schettini. A new method for rgb to xyz transformation based on pattern search optimization. IEEE Transactions on Consumer Electronics, 53(3):1020–1028, 2007.

[6] E. Bisong. Google colaboratory. In Building Machine Learning and Deep Learning Models on Google Cloud Platform, pages 59–64. Springer, 2019.

[7] A. P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. Pattern recognition, 30(7):1145– 1159, 1997.

[8] S. A. Burney and H. Tariq. K-means cluster analysis for image segmentation. International Journal of Computer App.lications, 96(4), 2014.

[9] M. A. Chandra and S. Bedi. Survey on svm and their application in image classification. International Journal of Information Technology, pages 1–11, 2018.

[10] L. de Oliveira Martins, G. B. Junior, A. C. Silva, A. C. de Paiva, and M. Gattass. Detection of masses in digital mammograms using kmeans and support vector machine. ELCVIA Electronic Letters on Computer Vision and Image Analysis, 8(2):39–50, 2009