ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 11 Issue 4 Nov 2023

SECURE CRYPTO-BIOMETRIC SYSTEM FOR CLOUD COMPUTING

Mr.K.V.Vara Prasad

ABSTRACT:

Cloud 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 cryptobiometric system applied to cloud computing in which no private biometric data are exposed.

INTRODUCTION

Cloud computing is a trend in application architecture and development, as well as a new business model. The success of many service providers, with Amazon as a remarkable example, has demonstrated that the model can be applied to a wide variety of solutions, covering the different levels defined in the cloud paradigm (SaaS, PaaS and IaaS). We can consider that cloud computing is at a mature stage, although there remain some limitations and challenges. Cloud computing brings important benefits for organizations that outsource data, applications, and infrastructure, at the cost of delegating data control. The information is processed in computers that the users do not own, operate, or manage. In this scenario, the user does not know how the

Assistant.Professor, Dept. of CSE,
Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

provider handles the information, and therefore a high level of trust is needed. The lack of control over physical and logical aspects of the system imposes profound changes in security and privacy procedures.

PURPOSE

The purpose of the project is to develop a secure crypto-biometric system for cloud computing. Cloud computing has become increasingly popular, enabling users to store and access their data remotely. However, security concerns have also risen due to the sensitive nature of the data being stored and transmitted. This project aims to address these concerns by combining the power of cryptography and biometric authentication.

The system will employ advanced cryptographic algorithms to ensure the confidentiality, integrity, and authenticity of the data stored in the cloud. These algorithms will encrypt the data before transmission and decrypt it upon retrieval, protecting it from unauthorized access or tampering. Additionally, the system will utilize biometric authentication techniques, such as fingerprint or iris scanning, to verify the identity of users accessing the cloud resources.

By integrating cryptography and biometrics, the system will provide a robust and multi-layered security framework. It will prevent unauthorized access to the cloud infrastructure and ensure that only authenticated individuals with verified biometric credentials can interact with the data stored in the cloud. This approach eliminates the risks associated with traditional password-based authentication systems, such as password cracking or sharing.

EXISTING SYSTEM:

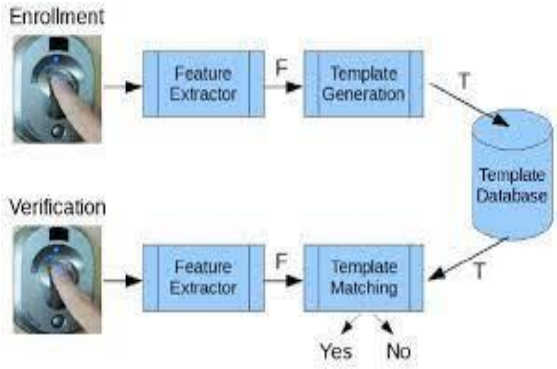
the data are stored in the user infrastructure, information location and protection mechanisms are known in detail. In contrast, a characteristic of public cloud computing services is that the user is completely unaware of data location. This makes it impossible to ensure that national compulsory regulations are met. For example, European data protection laws may impose extra constraints on the handling and processing of data that are transferred to the USA, so the use of Amazon S3 resources to store biometric templates could infringe the law. Several techniques have been proposed for biometric template protection. Among them, cancelable biometrics

ISSN2321-2152
www.ijmece .com
Vol 11 Issue 4 Nov 2023

[10] is one of the most promising. It satisfies a double goal: i) unrecoverability of the original biometric data from the stored biometric template (non-invertibility), and ii) the issue of a new biometric template when an existing template is compromised (renewability).

PROPOSED SYSTEM:

In the proposed schema, once a large database with sample acquisitions has been collected, an UBM can be trained. We propose the training methodology in Figure 3 (the addition of new UBMs) to improve the flexibility and security of our system. To train a new UBM, computing resources are provided by virtual machines hosted in Amazon EC2. The administration application requests from Amazon EC2 the required virtual machines automatically, using the API it provides. The training application and the new UBM are loaded and executed in the machines in a distributed way to reduce computation time. Speedup is possible due to the high parallelizability of the calculus performed on biometric data.



IMPLEMENTATION 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

ISSN2321-2152
www.ijmece .com
Vol 11 Issue 4 Nov 2023

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

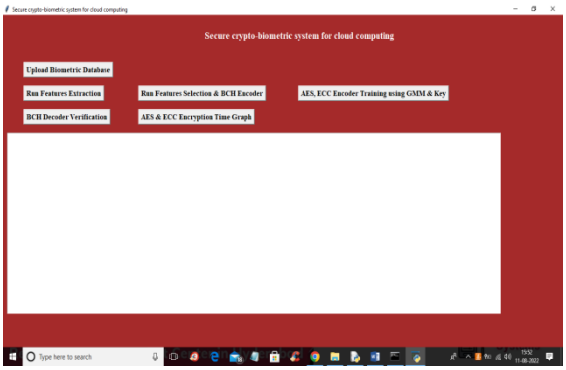
7) Comparison Graph:

using this module we will plot accuracy and other metric graphs

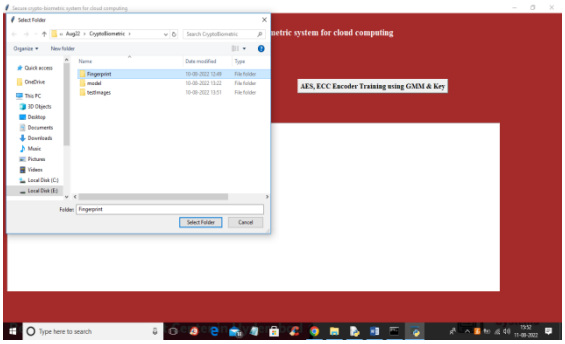
8) Predict Fish Status:

using this module we will upload test image and then SVM algorithm will predict whether image contains fresh or infected fish.

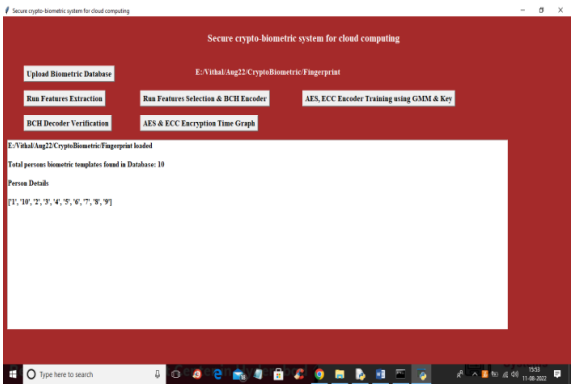
To run project double click on 'run.bat' file to get below screen



In above screen click on 'Upload Biometric Database' button to upload biometric data and get below output

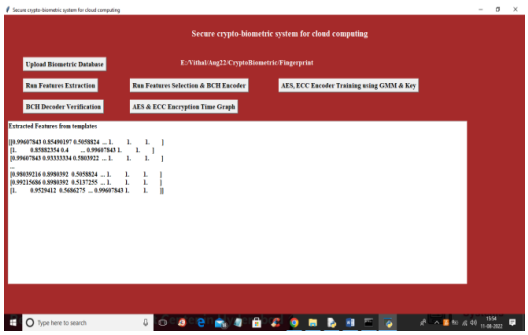


In above screen selecting and uploading Finger biometric images dataset and then click on 'Select Folder' button to load database and get below output

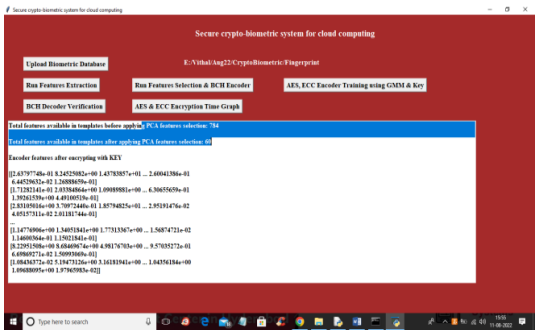


In above screen we can see database loaded and we can see it contains biometric template of 10 different

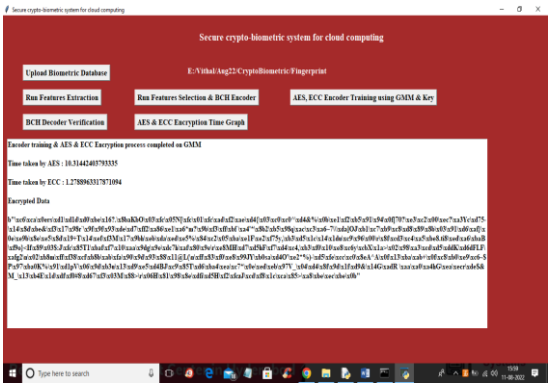
persons and now click on ‘Run Features Extraction’ button o extract features from templates and get below output



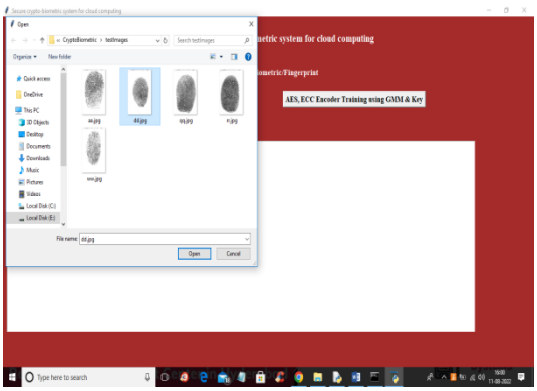
In above screen features extracted and now click on ‘Run Features Selection & BCH Encoder’ button to select features from extracted features



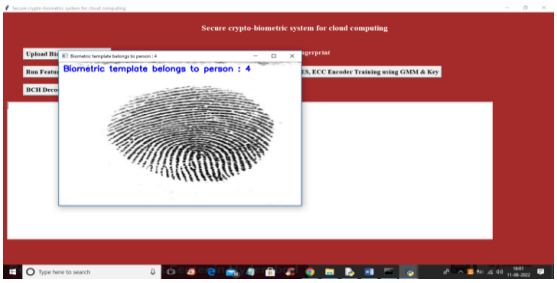
In above screen before applying PCA features selection algorithm, we have 784 features and then PCA select 60 important features out of it and now click on ‘AES, ECC Encoder Training using GMM & Key’ button to encode features and then train GMM and this GMM will get encrypted using ECC and AES algorithms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



In above screen GMM is encrypted and AES took 10.31 seconds and ECC tool 1.2 seconds and then we are seeing GMM encrypted data and now click on ‘BCH Decoder Verification’ button to upload template and get verification output

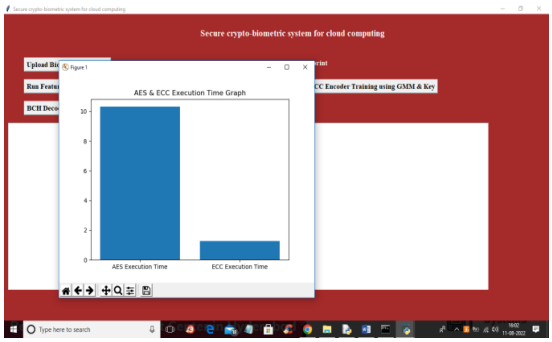


In above screen selecting and uploading finger template and then click on ‘Open’ button to get below output



ISSN2321-2152
www.ijmece .com
Vol 11 Issue 4 Nov 2023

In above screen template identified or belongs to person 4 and now click on ‘AES & ECC Encryption Time Graph’ button to get below graph



In above graph x-axis represents encryption algorithm names and y-axis represents execution time and in both algorithms ECC took less execution time.

CONCLUSION

In conclusion, the development of a secure crypto-biometric system for cloud computing offers a promising solution to address the growing concerns regarding data privacy and security. This innovative system combines the strength of cryptographic techniques with the unique characteristics of biometric authentication, resulting in a robust and reliable method for safeguarding sensitive information in cloud environments.By leveraging cryptographic algorithms, the system ensures that data transmitted to and stored in the cloud remains encrypted and inaccessible to unauthorized individuals. This provides a solid foundation for protecting the confidentiality and integrity of user data throughout the cloud computing process.Additionally, the integration of biometric authentication adds an extra layer of security by verifying the identity of users based on their unique physiological or behavioral traits. This mitigates the risks associated with password-based authentication, such as weak passwords or credential theft, significantly reducing the chances of unauthorized access to sensitive data.The secure crypto-biometric system not only enhances data security but also offers convenience and efficiency to users. By utilizing biometric characteristics like fingerprints or facial recognition, users can seamlessly authenticate themselves without the need to remember complex passwords, leading to a streamlined and user-friendly experience.Overall, the implementation of a secure crypto-biometric system for cloud computing addresses critical security concerns and ensures the protection of sensitive data. It paves the way for a more secure and trustworthy cloud computing environment, instilling confidence in

users and organizations alike.

REFERANCES

[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 Applications, 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.