Biometric Security for Cloud Data using Fingerprint and Palm Print

S.Sahithi, A.Anirudh, B.Swaroop, K.Ruth Ramya

Abstract: ***With the development of different multimedia services, Cloud-Based Multimedia System (CMS) is increasing its ubiquity. Web traffic is required to be ruled by the multimedia content by 72% by 2019. With such notoriety, CMS should be anchored, ought to give a proficient nature of administration, and ought to be adjusted. This paper gives a thorough survey of these attributes, going for the key plan contemplation's, for example, vigor, adaptability, accessibility, by and large execution. The way toward validating ourselves to machines is increasing day by day in the present coincided society. Well, known biometric approaches are palmprint and fingerprint recognition technology. Rather than utilizing palmprint acknowledgment or fingerprint acknowledgment framework independently for individual confirmation we can utilize both fingerprint and palmprint acknowledgment together to give an improved dimension of certainty for individual check and Identification.***

Keywords: ***Biometrics, Cloud data encryption, Palm Print, Fingerprint, Cloud security, Authentication.***

I. INTRODUCTION

Now a days computation over cloud storage has become a common thing for most of the applications. As the storage on local disks is unreliable in some cases, cloud-based storage is attracting everyone to store data on cloud which can be accessible everywhere. The number of individuals storing their data on cloud increases day by day, so the security level need to be in upgraded manner because when particular data is uploaded to the cloud the information is transparent to two parties. One is cloud services and the cloud administrator. Every will use their own encryption mechanisms and keys. By this many people think that our data is secured now, but no there is a chance to know our key. So keeping all these mechanisms a side there is another type of mechanism called user attribute-based encryption mechanism which uses the attributes of user in order to generate the key to encrypt their data in the storage. Within all the attributes provided we have selected the palm vein attribute.

II. CLOUD

It's nothing but a remote computational system which can store, manipulate the data. Majority of the users use their username and password for authentication purpose to store data but the main issue is that user can maintain too many accounts which leads to multiple access and either forgotten password or using same combo for various sites. In cloud computing protecting the data and various applications from unauthorized access is a major security concern. One of the greatest issue in cloud computing is the cloud contributor can also access the data of the authorized user. Securing our data is the major problem in cloud computing. We all use a local system for all our needs. If the system we are using crashes there will be no alternative for us to get back our data so, these days people are moving towards cloud services for storage of data where the it can be stored on multiple data servers. The data will be safe in other server even if one is crashed. As the cloud has advantages and many are using there will be more demand for that and many cloud provider companies were established and each cloud will be administered by its administrator.

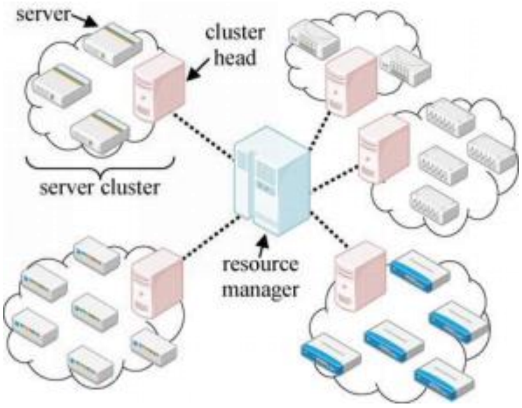


Fig.1. Centralized hierarchical of CBMS

III. FINGERPRINT

These days, fingerprint acknowledgment is a standout amongst all the most critical biometric advancements dependent on fingerprint uniqueness, ingenuity, and simplicity of obtaining. Despite the fact that there are numerous genuine applications utilizing this innovation, its issues are as yet not completely understood, particularly in low-quality fingerprint pictures and when ease securing gadgets with a little zone is embraced. In fingerprint acknowledgment process, the imperative advance which influences on framework precision is coordinating among format and inquiry fingerprint. Numerous arrangements are intended to expand this presently advanced precision.

Revised Manuscript Received on April 12, 2019.

S.Sahithi, Student, Department of Computer Science, Koneru Lakshmaiah Educational Foundation, Guntur. (Email: ammu1281998@gmail.com)

A.Anirudh, Student, Department of Computer Science, Koneru Lakshmaiah Educational Foundation, Guntur. (Email: anirudhmercedes11@gmail.com)

B.Swaroop, Student, Department of Computer Science, Koneru Lakshmaiah Educational Foundation, Guntur. (Email: swaroopsonu7@gmail.com)

K.Ruth Ramya, Assistant Professor, Department of Computer Science, Koneru Lakshmaiah Educational Foundation, Guntur. (Email: ramya_cse@kluniversity.in)y

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig 2 Sample Fingerprint

These coordinating calculations might be arranged into three sorts: particulars based methodology, connection based methodology and highlight based methodology. In any case, as dissected, the score of these calculations isn't high (particularly on the off chance that fingerprints are of a similar finger yet they are turned or the convergence is too little).

In this way, it's important to structure a model to institutionalized fingerprint layout with the end goal to enhance coordinating score.

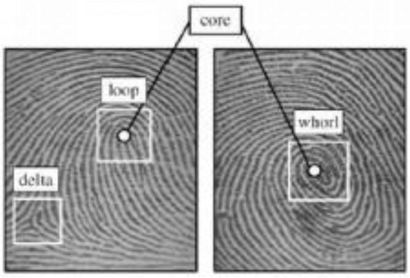


Fig.3 features of finger print image

IV. PALMPRINT

The most generally utilized biometric highlight is the unique mark and the most solid component is the iris. Anyway, it is exceptionally hard to extricate little one of a kind highlights, for example, details from misty fingerprints and the iris input gadgets are extremely costly. Other biometric highlights, for example, the face and voice are less exact and they can be emulated effortlessly. The palmprint is a generally new biometric include, has a few preferences contrasted and presently accessible highlights [1].The seven components influence the assurance of a biometric identifier in a specific application: comprehensiveness, uniqueness, Permanence, collectability, execution, agreeableness and circumvention. Palm print acknowledgment has been presented 10 years prior. It has progressively pulled in the consideration of different specialists because of its wealth in the measure of highlights. The Palm territory contains countless appeared in that can be utilized as biometric highlights, for example, Principal lines, geometry, wrinkle, delta point, details, datum point highlights, and surface [15].

In the wake of preprocessing of palm print images, highlights can be separated for matches. There are two kinds of acknowledgment calculations, check and distinguishing proof. In check, the framework approves a man's character by contrasting the caught biometric information and her own biometric formats put away in the framework database. The check is ordinarily utilized for constructive acknowledgment, where the point is to prevent various individuals from utilizing a similar personality. In distinguishing proof, the framework perceives a person via looking through the layouts of the considerable number of clients in the database for a match. Confirmation calculations must be precise. ID calculations must be precise and fast. Research on highlight extraction and coordinating techniques can be characterized into 4 classifications: Line-based, subspace-based, Statistical-based and coding based [5].

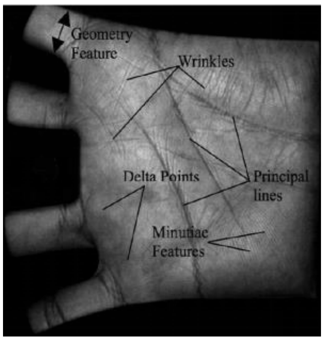


Fig. 4 Different Features of Palm.

V. LITERATURE SURVEY

P. Padma et.al.,[1] issued the essential paper on a wide range of biometric confirmation procedures in 2016. Finger Prints, Hand Geometry, Facial Image, Iris, Retina, Voice, Signature designs are the significant qualities of a man are associated with security methods at present. Mr. S.D. Raut et.al.,[3] distributed a paper on an audit of palm vein in which we will get an ideal clearness on how the palm veins are removed from our hand through the biometric sensor and the extent of the image, the beams entering into hand etc.,

G. S. Lipane1 et.al.,[5] gave us five kinds of methodologies for highlight extraction of palm print that is I) Line Based Approaches ii)Subspace Based Approaches iii)Statistical Approaches iv) Coding Approaches v) Fusion .

Dipti Verma1 et.al. [2] Composed an overview paper having a place with palm vein verification. It totally indicates how an image is prepared before particulars extraction. The procedure includes: - Thresholding (Removing Noise), Binarization and after that Feature extraction. The proposed strategy for Extraction of Minutiae is Crossing number Algorithm. It enables us to remove more properties on the veins. Yet, to get these properties unmistakably we should initially experience Hough change to discover the end focuses that will be utilized a while later for grouping.

Pranoti das et.al.,[14] also gave us the same methods given by [5] and explained the clear cut process from image acquisition till minutiae matching.

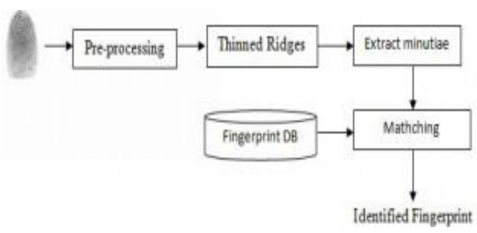


Fig 5 Fingerprint Recognition process

Ganesan and Tirthani have introduced the Diffie-Hellman Key Exchange calculation utilizing elliptic bend cryptography for a proficient exchange of encrypted data [4]. In this paper, they have utilized a customary one-level confirmation which is unsafe against security assaults.

Uma Somani et al. have executed the idea of RSA encryption along with the digital signature that outcomes in improving the information security of cloud in cloud computing [8].

Mona A. Ahmed, et.al presented the analysis of palm vein pattern Recognition techniques, methodologies, and systems. It talks about the specialized parts of ongoing methodologies for the following procedures; recognition of the region of interest (ROI), the segment of palm vein pattern, feature extraction, and matching [7].

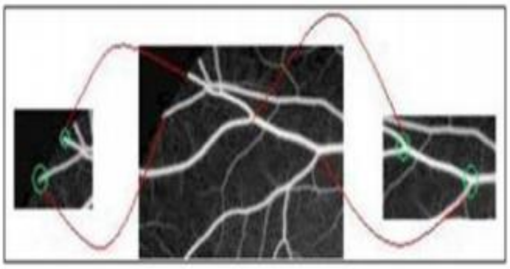


FIG 6. FINDING MINUTIA POINTS IN VEINS

R. Arun Prakashet.al., [9]. proposed a different methodology relating to encoding and encryption by using different types of methodologies in 2018. It helped us in the idea of the encryption process

Abdeljebar Mansouret.al., [10]. Provided us the basic ideas of multimodal biometrics for security to cloud data which was published in 2015.

P. Selvarani et.al. [11] Proposed a paper similar to multimodal biometric security but using the fingerprint and iris biometrics in 2018.

Alisherov, et.al. [12]. study explains to us that the palm print designs are inside to the body; it makes a troublesome strategy to manufacture. A palm print is another individual from biometrics family and attracts great part of the present research attention.

Rubina et.al. [13].. It gives the clear cut solution along with the formula and how to take ridge endings and bifurcations etc through CN algorithm.An author Tjokorda Agung Budi Wirayuda belonging to Indonesia also presented a paper (2015) .In this the calculation for false minutia is also given by a formula to be known. After calculating the minutia the matching techniques are also proposed.

Sumalatha et.al. [15] H in their reiew paper mentioned the basic methods of palm print recognition and its features which are used for minutiae extraction.

VI. PROCESSING OF IMAGE

The image acquired will be further processed inorder to identify the features of the palm vein obtained [15].

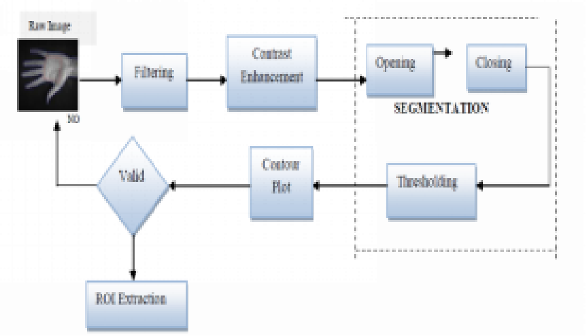


Fig 7. Basic steps of preprocessing

VII. FILTERING

The clarity in a particular image varies from one to another. Thus, to extract the features the structure of the palm veins in the image must be perfect enough to identify. Basically, linear filters and nonlinear filters are the types of filters we commonly used to reduce the noise of an image. But every filter has its role in image processing functions. Different filters are used for different type of noises. It depends on the nature of noise in it and the image data to use which type of filter [3].

VIII. CONSTRAST ENHANCEMENT

The usage of IR image will lead us to further improve the clarity that is contrast of image before segmenting. These can be done by histogram or adaptive methods. So basically in this part the contrast that appeared all over the image will be adjusted.

IX. EXTRACTION OF CENTER POSITIONS OF IMAGES:

The image is converted as a cross-sectional profile which is it is divided into several profiles on the vertical axis. Then by calculating the maximum point from the curve taken from the profile histogram the center point is noted.

X. ROI EXTRACTION:

Basically some algorithms are used for ROI extraction that is region of interest. By extraction this region from the image obtained after extraction of center positions, finding of minutia will become easier. Because it gives us the important region where we can easily detect the minutia.

XI. METHODS FOR MINUTIAE EXTRACTION

A great quality image is significant for details extraction. In any case, some of the time the image quality may be poor because of different reasons and thus it winds up important to improve the fingerprint images before particulars coordinating of fingerprints. The particulars extraction strategies are characterized into two general classes. Techniques that chip away at binarized fingerprint images:

- Techniques that work specifically on dim scale fingerprint images.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- Given beneath is a chart demonstrating the diverse classifications of details extraction procedures? The accompanying subsections will examine the above strategies intricately.

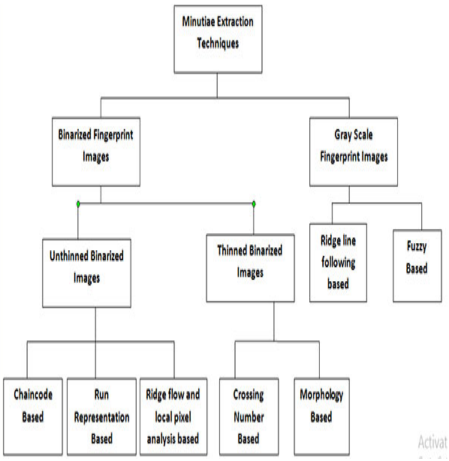

Minutiae Extraction Techniques
Binarized Fingerprint Images
Gray Scale Fingerprint Images
Unthinned Binarized Images
Thinned Binarized Images
Ridge line following based
Fuzzy Based
Chaincode Based
Run Representation Based
Ridge flow and local pixel analysis based
Crossing Number Based
Morphology Based

Fig 8: Classification of Minutiae Extraction Techniques

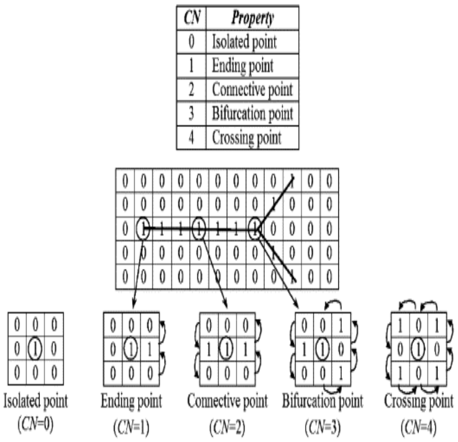
As there are many techniques for minutiae extraction we mainly choosen and moved on with cross number based technique as it gives the accurate minutiae points.

Crossing number based

Intersection number based is the most generally utilized strategy for details extraction in the diminished binarized images class. It is preferred over different techniques as a result of its computational effectiveness and characteristic straightforwardness [13]. In this technique, a skeleton image is utilized where the edge stream design is eight-associated. As appeared in the figure underneath, the nearby neighborhood of each edge pixel in the image is examined utilizing a 3×3 window from which the particulars are removed. The intersection number esteem is processed. The intersection number properties can be utilized to arrange an edge pixel as a closure, bifurcation or non-details point. Figure beneath demonstrates the intersection number properties [16].

$$CN = 0.5\sum_{i=1}^{8} | P_i - P_{i+1} |$$

Fig:9 Formula of CN



CN	Property
0	Isolated point
1	Ending point
2	Connective point
3	Bifurcation point
4	Crossing point

Fig 10. Properties in cross number and Finding CN points using matrix

For example, let us assume that the value of CN=0 according to the ridge, this will represents to an isolated point and a CN of 4 corresponds to a crossing point [13]. Similarly if CN=1 that is end point of the line, if CN=2 then it is called as the connective point of two lines and at last if CN=3 it is the bifurcation point of the ridge where divide into two.

proposed model

First block is for the enrollment procedure; for enlistment an interface will be given to user at the interface a scanner is there to examine the fingerprint and palm print a quality checker will check the nature of prints which has been taken from the user here minutiae and wrinkles is the features of fingers and palm, hash code is produced from extricated highlights of palm and fingers at that point put away in the databases. In check process the client who need to confirm himself needs to filter his hand and a hash code is created from the examined prints then that hash code is contrasted and the recently put away one hash of that client on the off chance that the hash is coordinated, the requester is a real client generally not a genuine client.

This framework has two module initially is enrollment and the second one is confirmation.

A. Registration:

Step-1: A contactless acknowledgment framework checks (read) minutiae (where edges of fingers and lines end or edges split in two) from fingers and wrinkles from palm (computerized palmprint acknowledgment framework).

Step-2: from examined fingerprints and palm print, a hash code is produced and put away to the diverse databases.

B. Verification:

Step-1: Scans minutiae from fingers and wrinkles from palm through an optical sensor.

Step-2: After the checking procedure, a hash code is produced from examined biometric.

Step-3: Firstly hash code of newly obtained palmprint and hash code of palmprint which is already stored is compared.

I. In the event that both hash codes are not coordinated, the demand of confirmation is dropped.

ii. Else it is sent to the next stage.

Step-4: Comparison between the hash code of newly obtained fingerprint and hash code of fingerprint which is already stored is performed.

I. On the off chance that hash codes are not coordinated, the demand of check is dropped.

ii. Else verification process is finished.

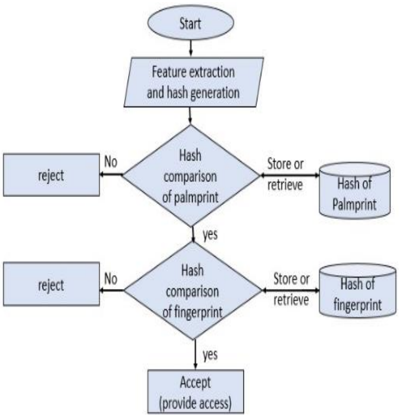


Fig 11: Flow Chart of palmprint and fingerprint recognition.

XII. ENCRYPTION TECHNIQUES

AES ALGORITHM for encryption

Rijndael is used for securing information. it is also called as Advanced Encryption Standard (AES). AES is a symmetric block cipher that has been utilized generally these days. On the off chance that a client needs to store his/her information in the cloud through Cloud Service Provider (CSP) the client presents their prerequisites and picks best-indicated administrations offered by the provider. At the point when the information is moved to the picked CSP occurs and in future at any point if the user uploads any information in the cloud, the information will initially be encrypted using the AES algorithm and after that sent to the provider. The information is transferred on the cloud after its encryption, any demand to peruse the information will happen after it is decrypted on the client's end and after that the plain content information can be perused by the client. This incorporates a wide range of information. This encryption is straightforward to the application and can be coordinated rapidly and effectively with no progressions to the application. Since it might bargain the key additionally, the key is never put away alongside the encoded information. A physical key administration server can be introduced in the client's premises so as to store the keys. This encryption assurances to secure information and keys that they stay under client's control and will never be exposed in storage or in transit [9].

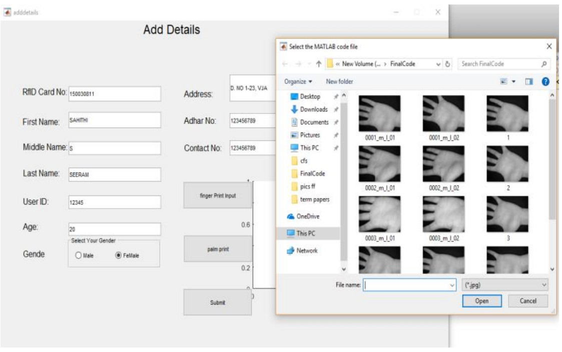
DIFFIE-HELLMAN for key exchange

It is a specific algorithm for exchanging cryptographic keys. It is a standout amongst the most prompt realistic models of key exchange in the field of cryptography. The Diffie– Hellman key exchange system grants two social affairs that have no prior learning of each other to together set up a shared secret key over a questionable correspondences channel.

This key would then have the capacity to be used to scramble subsequent trades using a symmetric key figure. The arrangement was first dispersed by Whitfield Diffie and Martin Hellman in 1976, regardless of the way that it had been freely built up several years sooner inside GCHQ, the British signs knowledge office, by James H. Ellis, Clifford Cocks, and Malcolm J. Williamson, notwithstanding, was kept classified.[citation needed] In 2002, Hellman proposed the estimation be called Diffie– Hellman– Merkle enter the exchange affirmation of Markel's duty to the advancement of open key cryptography.

XIII. RESULTS

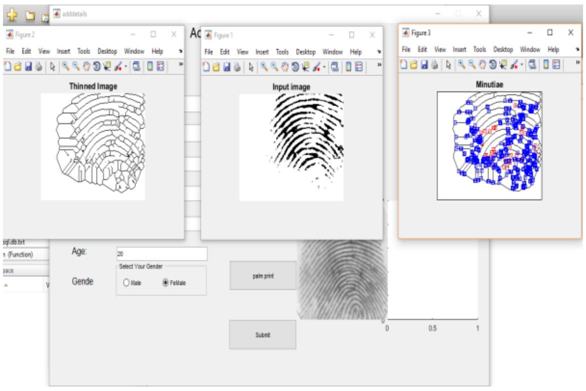
Registering of user


adddetails

Add Details

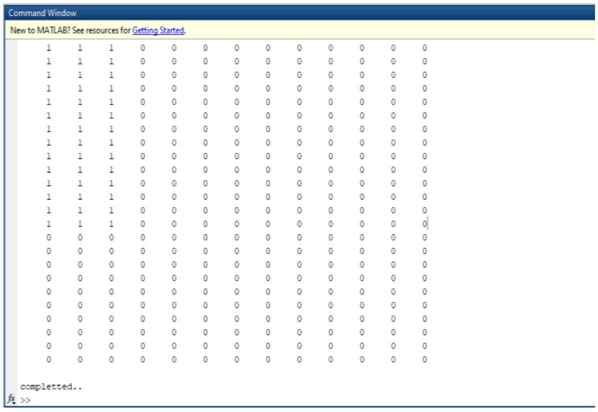
RfID Card No: 150030811
First Name: SAHITHI
Middle Name: s
Last Name: SEERAM
User ID: 12345
Age: 20
Gende Select Your Gender ○ Male ● FeMale
Address: D. NO 1-23, VJA
Adhar No: 123456789
Contact No: 123456789

Fig 12. Adding of finger print and palm print images



Age: 20
Gende Select Your Gender ○ Male ● FeMale

Fig 13. Minutiae generation of finger print image


Command Window

New to MATLAB? See resources for Getting Started.

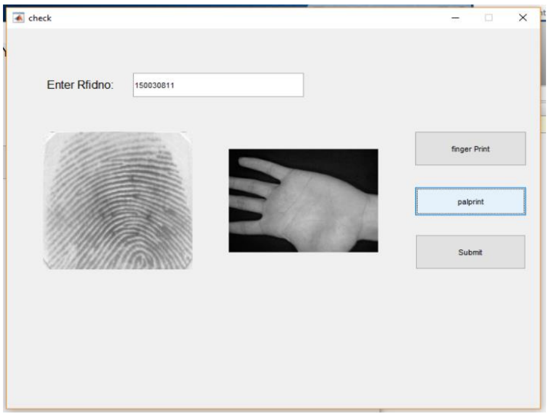
```
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     1     1     1     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0
     0     0     0     0     0     0     0     0     0     0     0     0     0

completted..
fx >>
```

Fig 14. Conversion of minutiae points to binary

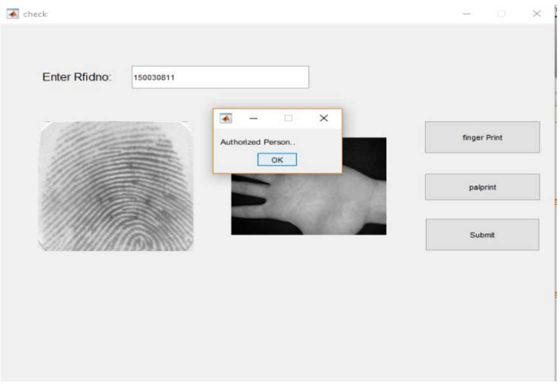
Verification of user

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication


check

Enter Rfidno: 150030811

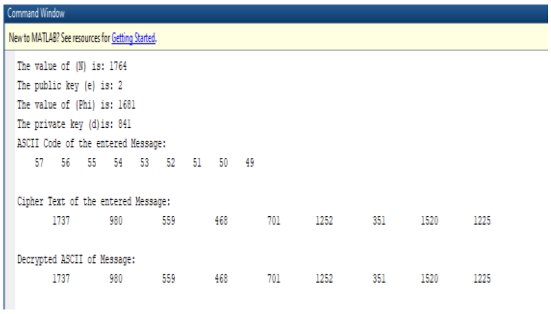
Fig 15. Aubmission of details for verification


check

Enter Rfidno: 150030811

Authorized Person..

Fig 16. Message of authorization


Command Window

New to MATLAB? See resources for Getting Started.

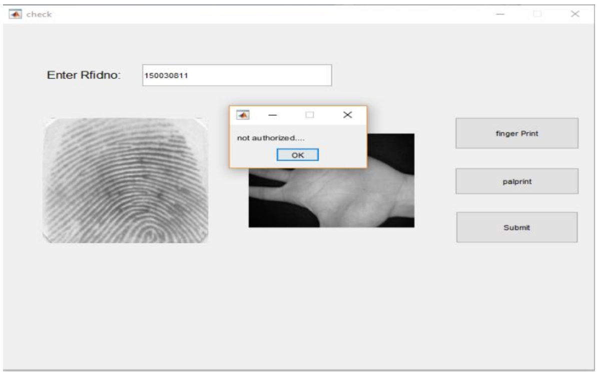
```
The value of (N) is: 1764
The public key (e) is: 2
The value of (Phi) is: 1681
The private key (d)is: 841
ASCII Code of the entered Message:
    57    56    55    54    53    52    51    50    49

Cipher Text of the entered Message:
        1737         980         559         468         701        1252         351        1520        1225

Decrypted ASCII of Message:
        1737         980         559         468         701        1252         351        1520        1225
```

Fig 17. Hackground process of encryption and decryption of users details

If the person details do not match under the details of the particular id then he is given as not authorized person and no data will be shown for him.


check

Enter Rfidno: 150030811

not authorized....

Fig 18. Unauthorized prompt

XIV. CONCLUSION

Even though the authentication is done and cloud access is granted to the user the data needed to be decrypted in order to get original data. If the given or considered fingerprint or palm print does not match the data decrypted will also goes wrong and raw data will not be exposed to no one except the owner of that data. Multimodal biometrics are now cherishing than any single biometric system authentication. So, the combination of finger print and palm print gives us a great combination.

REFERENCES

1. P. Padma and Dr. S. Srinivasan issued a the basic paper "A survey on Biometric Based Authentication in cloud computing" in 2016.
2. "A SURVEY ON BIOMETRIC AUTHENTICATION TECHNIQUES USING PALM FEATURE", Dipti Verma, Dr.Sipi Dubey in 2014.
3. "Review of Biometrics: Palm Vein Recognition System ", Mr. S.D. Raut 1 and Dr. V.T. Humbe 2,Issue-1,March 2014.
4. Tirthani, N., Ganesan, R.: "Data security in cloud architecture based on Diffie hellman and elliptical curve cryptography IACR Cryptology", ePrint Archive 49 (2014)[5] "Palm Print Recognition Review Paper" ,G. S. Lipane 1 , S. B. Gundre 2,2014.
5. "Fingerprint recognition using standardized fingerprint model", Le Hoang Thai and Ha Nhat Tam ,IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.
6. Mona A. Ahmed, Hala M. Ebied, El-Sayed M. El- Horbaty, Abdel-Badeeh M. Salem (2013) 'Analysis of Palm Vein Pattern Recognition Algorithms and Systems' International Journal of Bio-Medical Informatics and e- Health Volume 1, No.136
7. Somani, U., Lakhani, K., Mundra, "Implementing the Digital Signature with RSA Encryption algorithm to Enhance the Data Security of cloud in cloud computing" IEEE (2010).
8. "Biometric Encoding and Biometric Authentication (beba) Protocol for Secure Cloud in M-Commerce Environment" by R. ArunPrakash , T. Jayasankar and K. Vinothkumar in 2018.
9. "A Context-Aware Multimodal Biometric Authentication for Cloud-Empowered Systems" by Abdeljebar Mansour, Mohamed Sadik , Essaïd Sabir , and Mohamed Azmi in 2016.
10. "To Enhance the Data Security in Cloud Computing Using Multimodal Biometric System" P. Selvarani, N.Malarvizhi in 2018.
11. Alisherov, F., Kim, T., Sarkar, I., and Bhattacharyya, D. (2010),Palm Vein Authentication System: a Review, International Journal of Control Automation.
12. Arati A.Yadav 1 , Dhanashree P.Patankar 2 , Rubina S.Nandrekar 3 ,"Analysis And Detection of Ridge Ending For Person Identification System " in 2016.
13. Pranati Das and Sachin meshram "A Review Paper Based On Palmprint Recognition System" in 2014.
14. Sumalatha K.A, Harsha H "Biometric Palmprint Recognition System: A Review" in 2014.
15. "Palm Vein Recognition Based-on Minutiae Feature and Feature Matching" , Tjokorda Agung Budi Wirayuda ,August 10-11, 2015, Bali, Indonesia. https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication