BIOMETRIC SECURITY FOR CLOUD DATA USING FINGERPRINT

J. Vimal Rosy

Head, Dept. of Comp. Science

Soka Ikeda College of Arts and Science for Women,Chennai

Dr. S. Britto Ramesh Kumar

Asst. Prof., Dept. of Comp. Science

St. Joseph's College, Tiruchirappalli

Abstract

The most important phenomena in the cloud is nothing but security of confidential business data and it is sure that only authenticated and authorized personnel can have access the data and applications in the cloud. It is the frightening security risk and a threat between the users both to a distant server away from the direct control of the user. It will be deeply analyzed, in the paper, the use of biometric authentication in cloud computing. It opens a new way to help reducing the security threats. The reason is this that the provision of biometric authentication seems to be comprehensive and structured overview for the enhancing security in the cloud.

Keywords: Cloud Computing, Biometrics, fingerprint, Cloud Security, Authentication

I. Introduction

The astonishing factor that shaking up the transactions in cloud computing is only the security and the anxiety of the researches and technologists to match a solution to the challenges ahead between the provider and the user. In an on-demand environment cloud computing fulfills the request of the multitenant for services and resources demanded from the service provider. Thus, the users can have access services according to the needs. They may not know the persons or places delivered to them.

It is a fact that the strength of the individuals increases day by day and so the data too. Accordingly, the level in security must come up. When service providers share and maintain the client data. It should be free from threats and leaks in data. Several mechanisms tried on data security, but many failed to secure security.

In a way authentication which have come to help ensure and confirm a user privacy. The existing traditional technology by a password authentication is not at all successful with limitations. So, the biometric authentication which is physical based biometric authentication and based on behavioral biometric authentication seems to be lessening troubles in security.

II. Biometric Authentication

Biometric is an emerging technology which is a computerized method of identifying a person of his physiological characteristics. It proves to be a promising method for authentication in a cloud environment to make sure of clear security in cloud computing.

III. Literature Review

The importance of cloud computing security and techniques to overcome data privacy issues and the rising problems while handling in cloud service provider author in (1) gives a solution in block chain community. Relating to industry glitches are analyzed from organizing new cryptographic primitives.

Author in (2) came with a proposal of two methods in order to secure data using fuzzy vault technique to rehearse error- correcting codes in the secret key when false identification is used by the invader. But a highly expensive system is required to conformist cryptographic primitives.

Author in (3) tries to explain multiple methods to secure data in comparison with Cryptography methods. It requires real time analysis for better results because the multimedia data are high dismissal of large capacities.

Author in (4) proposed a protective biometric identification. It is a hybrid of cognitive and quantum cryptography. The data are stored in DNA storages inside the cloud still it is difficult to overcome DNA storage limitations by storing biometric templates in cloud DNA database.

Author in (5) introduces the bases of fingerprint authentication. AES algorithm for encryption and Diffie-Hellman for key exchange can be used. The usage of phalange prints as a emerging means of authentication. Finally, multi model biometrics are more desirable than any single biometric system authentication. The best is the combination of finger print and palm print combination to attack conspiracy tossed by the users and the cloud server. The most important phenomena in the cloud is nothing but security of confidential business data and it is sure that only authenticated and authorized personal can have access the data and applications in the cloud. It is the frightening security risk and a threat between the users both to a distant server away from the direct control of the user.

It will be deeply analyzed, in the paper, the use of biometric authentication in cloud computing. It opens a new way to help reducing the security threats. The reason is this that the provision of biometric authentication seems to be comprehensive and structured overview for the enhancing security in the cloud.

IV. Fingerprint

Human creation has given us a highly unique feature in finger as no two individuals own the same finger print, so it is a remarkable proof of characteristics in individual identity technology. Fingerprint technique is almost successful in various applications such as in the forensic, government and civilian domains. The criminals unknowingly leave their fingerprint where crimes take place. It also needs the existence of large legacy databases to store them. So, it is very difficult to allot compact and inexpensive fingerprint readers.

If fingerprint is to be recognized in two ways for verification and identification. In verifying the fingerprint an input fingerprint is to be compared with the enrolled fingerprint of the particular user to find out whether they are the same finger (1:1) match and identified with the original.

V. Problem Statement

The three different components sensor in biometric system are recording the information, a computer for storing biometric information and a software that connects computer hardware to the sensor.

As it is crystal-clear that security is the major problem for biometric. The service providers of the cloud store and maintain the data of the client across data centers and they also fall into threads of leakage of data. The fingerprint converted into pixels with accurate point.

Suppose the attacker hack the fingerprint sometimes the pixels may be changed and do not match with the original. So, it is a drawback in biometric authentication.

VI.Proposed Model

As soon as the finger print is registered is being converted into QR code and saved. Each image has its own QR code. The following authentication mechanism is illustrated.

The authentication mechanism with biometric in cloud divided into 3 phases.

1.Enrolment Phase
2. Login Phase
3.Authentication Phase

i. Enrolment Phase:

- The first phase is the enrolment phase when a user wants to use the cloud service registers one‘s biometric details with the cloud computing server.
- Through a fingerprint scanner one’s fingerprint is captured.
- The quality of the image is checked.
- Then extract the feature of the biometric data.
- A unique QR Code is generated for identification.
- The QR code is stored.
- The feature is encrypted by the public key got from cloud server.
- It is to be sent to the cloud server after encryption.
- It is stored in the cloud database.

ii. Login Phase:

- The biometric data is captured from the user for authentication.
- Compare the extracted feature.
- The QR code is calculated for identification.
- Using the public key, the extracted template is encrypted.
- The extract template is sent to the server-side post encryption.
- Decrypt the feature template.
- The encrypted template is retrieved form the database.

iii. Authentication Phase:

- With the help of web API in the retrieved of the template which is stored in the cloud and it acts as a link between the user interface and the cloud server.

- The store biometric template is encrypted.
- It is compared.
- In case it matches, authenticate the use to access the cloud service.
- Otherwise, send back the user to login session with proper message.

The structure of Biometric system process as shown in fig 1.1.

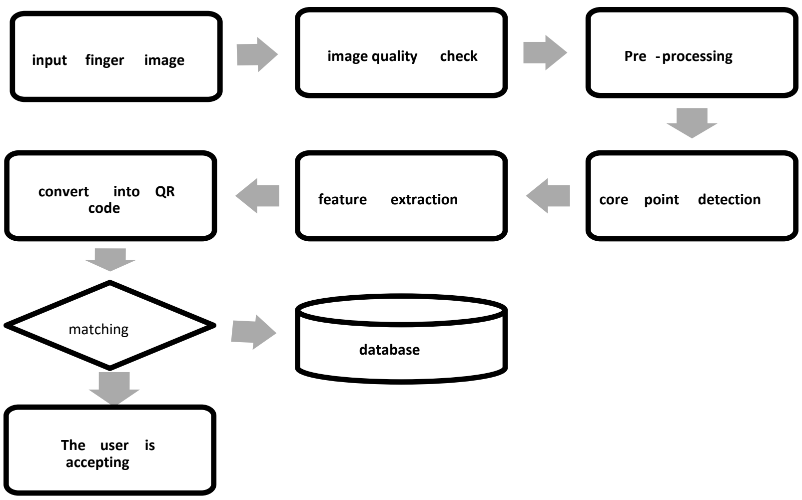


Fig 1.1 Bio-metric Process Pre-processing:

Preprocessing is a technique for correcting distortions, crop and mark the regions of interest for the sake of feature extraction. Preprocessing falls under six steps. The figure 1.3 shows the steps of preprocessing.

1. convert to Gray-scale
2. Edge enhancement:
3. Filtering
4. Binarization
5. Thinning
6. Minutiae extraction **Conversion to Gray Scale:**

It is necessary that RGB is converted into gray scale.

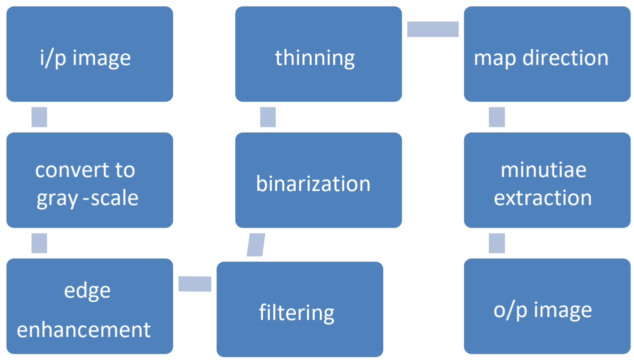
Edge Enhancement:

While taking into consideration each finger-print image, it is segmented and the same is classified into:

- well defined Region

- Recoverable Region
- Unrecoverable Region

Fig 1.2 Fingerprint Recognition process



Thinning:

The width of the ridges is reduced to one pixel. Example Skeletons, spikes. Fill up holes, into small breaks, eliminating bridges, ridges etc.

Binarization:

By this process, it is converted into 8bit gray scale fingerprint image into a 1-bit ridge image for convenience, it is equivalent to thresholding, post-processing for the binarizing image like smoothing is important in this process.

Filtering:

As it is true that a image is different from another in clarity. For identification, the perfection of the structure of the image must be reached. In order to reduce the noise of an image, linear filters and non-linear filters are used in common. Because each filter has its own processing functions.

Methods for Minutiae Extraction:

When an image is extracted it is significant to note a good quality of the image. Sometimes the quality of the image may be poor due to many reasons. So, the fingerprint images should be improved before co-ordination. The extraction strategies fall into two general classes. During binarized level, techniques may chip away.

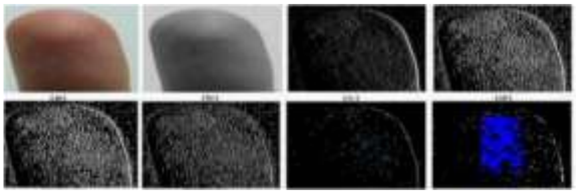


Fig 1.3 Basic steps of preprocessing Encryption Techniques:

Asymmetric or public key cryptography uses two keys, namely one public key to encrypt data and the other private one to decrypt data as per of, the principle of substitution permutation network.

Since AES computers on bytes, it treats all the bits as bytes. For example, 128 bits are treated as 16 bytes using AES algorithm on 4*4 matrix.

Encryption Process:

The process consists of four sub process in one round. The first one is depicted below:

Byte Substitution:

The 16 input bytes are substituted in a permanent table (8-box) refer design. Thus, the outcome is in matrix of four rows and four columns accordingly.

Shift rows:

Entire four rows of the matrix are shifted to the left. If any entry which falls off are reinserted on the right side of the row in matrix.

The following way is done in shift:

- Matrix first row remains the same.
- Second row is then shifted by one
  (byte) place to the left.
- Likewise in third row of the matrix shifting is dine two positions to the left.

- Three positions to the left are shifted in the fourth row.
- Now a new matrix is formed with the same 16 bytes but are shifted with the value to each other.

Mix Columns:

By an special mathematical function an alteration is done in each column of four bytes. Thus this function takes as input the four bytes of one column and outputs of four new different bytes replacing the original column. The result is the formation of different new matrix of the 16 bytes. At the same time remember that this measure is not repeated in the last round.

Conclusion:

In fine, two concepts are involved in CC one is sharing and the second is payment for using respectively. Computing services are IaaS, SaaS, and PaaS. Therefore, it is most necessary to allow only authorized users to have access to expected services in cloud. So, unless authentication is secure, cloud services cannot be provided to the authorized user apart from the traditional techniques for authentication like password, OTP, etc. are a better option is recommended to use biometric authentication to overcome the drawbacks of password technique which may be stolen by hackers or forgetting of the password indulges into trouble. So, only the biometric authentication system with QR code some improvement can give security level of cloud provider conveniently.

References

1.H. Halpin and M. Piekarska, “Introduction
to Security and Privacy on the Blockchain,”
2017, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris,2017, pp 1-3.

2.I. Zhu, C, Zhang, C, Xu, X. Liu and C. Huang, “An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing,” in IEEE Access, vol. 6, pp. 19025-19033, 2018

3.Mehreen Ansar, Muhammad Sheraz
Arshad Malik, Mubeen Fatima, SadafAslam, Anum Rasheed, IqraNazir, "Biometric Encryption in Cloud Computing: A
Systematic Review", IJCSNS International Journal of Computer Science and Network Security, VOL..18 No.8, August 2018.

4.S. Sahithi, A.Anirudh, B. Swaroop,K.Ruth
Ramya, "Biometric Security for Cloud Data using Fingerprint and Palm Print", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8,
Issue-6S3, April 2019.

5. Zarnab Khalid, Muhammad Rizwan, AyshaShabbir, Maryam Shabbir, Fahad Ahmad, JaweriaManzoor, "Cloud Server Security using
Bio-Cryptography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10. No.3.2019.

6. Kok-Seng Wong* and Myung Ho Kim,
"Secure Biometric-Based Authentication for
Cloud Computing",I. Ivanov et al. (Eds.): CLOSER 2012, CCIS 367, pp. 86–101, 2013. © Springer International Publishing Switzerland 2013.

7. W.K. Hassan, H. Al-Assam, Key exchange using biometric identity based encryption for sharing encrypted data in cloud environment. In Proc. SPIE 10221, Mobile Multimedia/ Image Processing, Security, and Applications, 2017.

8. P. Padma and Dr. S. Srinivasan issued a the basic paper "A survey on Biometric Based Authentication in cloud computing" in 2016

9. P. Selvarani, N.Malarvizhi in 2018, "To Enhance the Data Security in Cloud Computing
Using Multimodal Biometric System."

10. S. Ilankumaran and C. Deisy, "Multibiometric authentication system using finger vein and iris in cloud computing," Cluster Comput., pp. 1–15, 2018.

11. "2030 Vision Goals," 2018. [Online]. Available: http://vision2030.gov.sa/en/goals. [Accessed: 29-Sep-2018]

12. S. Barra, K.-K. R. Choo, M. Nappi, A. Castiglione, F. Narducci, and R. Ranjan, “Biometrics-as-a-Service: CloudBased Technology, Systems, and Applications,” IEEE Cloud Comput., vol. 5, no. 4, pp. 33 – 37, 2018.