Security of a Biometric Template in Cloud Computing

Madhu Chauhan

December 8, 2019

SECURITY OF A BIOMETRIC TEMPLATE IN CLOUD COMPUTING

Abstract- Cloud computing is in the air nowadays. Almost every organization, industry and institute has either already implemented or in the phase of implementation of cloud and are trying to make out full benefit out of it. This is one of the most secure and optimized method to store data and applications. Whenever one talks about securely retrieving the data, the techniques that come to mind are: token based, password based, digital signature and Biometrics. In this paper, all these methods are briefy described by putting more emphasis on biometrics. Under the umbrella term biometrics, fingerprints are most widely used to access data and applications securely thereby minimizing the errors. Now if fingerprint is so vital, it is important secure a fingerprint sample also. This paper describes various already existing techniques to secure fingerprint and proposes a more optimized one.

Keywords: Biometrics, minutiae points, preprocessing, cloud, authentication

I. INTRODUCTION

The term cloud computing has totally revolutionized the world of computing. It has become the choice and rather need in different fields of application. There are numerous types of clouds mainly private cloud, public cloud and hybrid cloud. The data stored on these clouds can be securely accessed as and when required. For this purpose, various methods of authentication are discussed later on. If one talks about use of biometric systems on cloud, it is feasible. Out of all the traits that are studied under biometrics, fingerprint is most widely used which portrays a unique combination or ridges and valleys. No persons can have same fingerprints.

Initially, user provides a fingerprint sample. These samples are stored on the cloud. Whenever user requires any kind of resource from the cloud he has to scan finger against sensor. This sample is then compared with the one stored on the cloud first.

On proper match the user is given the access to the requested resource. While sending the sample on cloud the sample has to be encrypted for security purpose. This is how the biometric system is implemented on cloud.

A. *Overview of existing methods of Authentication*

1) *Password Based:* This is one of the most trusted and traditional methods for authenticating a genuine user. Even though most organizations have done a great work in making the password more secure by either increasing the number of characters or by making a compulsion of adding special characters in the password. But unfortunately, attackers are competent enough to crack them.

2) *One time password:* In this method, the user registers himself by providing e-mail id or contact number. The one time password is sent on either of them. The drawback of this method is that a token is gerenerated with every transaction which inturn increases the overhead.

3) *Digital Signature:* In this mechanism, a digital signature is generated by user on the basis of user’s name, date of birth etc. This digital signature is sent to others at the time registration. In case, this digital signature is spoofed by some unautharized person, all the hardwork goes useless.

4) *Biometrics: More Secure than Traditional Authentication Methods*

Every person has his own unique biometric traits. This unique identity is used for the purpose of identification and authentication. The major benefit of using biometrics is that it can not be duplicated and is successful to a very large extent in almost all the application areas.

A new term is deviced as- Cloud Biometrics, which is available on demand. These are managed and maintained by cloud service providers. As we know that biometric template is recorded at the time of enrollment. The template database may contain a millions records and could be geographically distributed.

The template-fingerprint, is a key to access many resources from the cloud. For the purpose of authentication, fingerprint templates of various users are stored in the database, which is matched with template of actual user at the time of data retrieval.

B. *Need for encryption*

A question comes to our mind-"Is a Biometric sample secure?"

Fingerprints are used in different sectors for multiple purposes depending upon the applicability. A fingerprint can be used for the purpose of attendance, in various government offices and private institutes.

A fingerprint can also be used for securing any confidential data or file saved in the phone or desktop. Also, a fingerprint can also be used as authentication tool for laptops or other digital devices.

Another use of finger print could be to secure any particular area where some confidential files are lying or some weapon or antique item is placed. This particular could only be approached by authenticated people when they provide their fingerprint on the sensor. Any other person would not be able to enter in that area.

A fingerprint can also be used for the purpose of identification of a criminal, where the criminal has left some print of finger on any particular item.

When a fingerprint is so important and useful tool for the purpose of security, then this fingerprint itself should also be made secure so that it could not be copied or manipulated by any intruder for any illegal purpose. Consider the case where one is sending the fingerprint data for the purpose of identification of a criminal and this sample is tampered in between. Or one is sending fingerprint details of a very important person for the purpose of remote login or remote access of some resource. It may also happen that any intruder access the data stored on cloud by getting the access of legitimates fingerprint sample. Therefore, it is important to have foolproof mechanism for securing fingerprints.

Maintaining the security of the templates stored in database is crucial if the biometric system is to be implemented on cloud and made robust. Although, these templates are unique in nature, but still they can be hacked and misused for some illegal purpose. There is a need to encrypt the biometric trait. The encryption algorithm, encrypt the fingerprint sample for accessing any document of file from the cloud. Here, even if the hacker gets the control of database of all the fingerprint templates, it will be of no use as the samples are encrypted.

With above discussion, it is analysed that one must effectively guard against vulnerabilities. To achieve this, a template-protection strategy should be thought of. There are many fingerprint encryption techniques, some of which are discussed in literature review.

II LITERATURE REVIEW

Jain et al. [1] emphasised upon the fact that biometric techniques are preferred against other tradtional techniques. Again, boimetric systems are threat prone. Among all the types of attacks and threats author identified that securing a strored template is at utmost priority. Authors gave a detailed description of numerous schemes that are currently in use for securing a biometric template along with their impact, advanteges and disadvanages to combat against incresed number of threats involved with the technology. After in depth analysis, he identified most of the schemes are not capable enough to work for large-scale data and are based on brute force attacks that works on the prerequisite of uniformity of biometric features. He also discussed fuzzy vault scheme that is based on cryptoanalysis. He recommended using hybrid techniques to make the biometric templates intact.

Jain et al. [2], in their paper stressed upon the fact thet identity of human being must be kept at utmost priority specifically in the application areas where wrong identification can lead to blunders like at airports, passport offices and security agencies and many more. Authors discussed the loopholes present in existing traditional system and stated traditional identification methods like password and tokens as unreliable. They advised that use of biomertic traits for the purpose of identification and verification are much more secure and less vulnerable to attacks. An amalgamation of traditional and biometric system could also be used.

Ansar et al. [3] state the fact that biometrics have proved themselves as the better approach in the world of security. Their concern is about security of a Biometric trait template in the databases stored on clouds. Although many techniques exists that works upon extraction, storage and secuty of the templates but pros and cons are associated with every method. Authors suggest a highly secured technique known by the name of Biometric Cryptosystem in which the template is encrypted using an encryption technique. The process of encryption consists of few steps namely sensors, signal processing, cryptography approach, Quantum cryptography, and Cognitive cryptography, storage of template, Cognitive Cryptography, merger, pattern matching and decisions. In addition to this, a key is generated which is attached to the template itself thereby creating helper data. This helper data is the one, which is visible to general public hiding the original template.Quantization process was also been used during key generation process.

According to authors, in cognitive cryptography, the object is divided into various parts and then secured seperately. But in this technique is not suitable for high level security and less optimized in terms of size, cost and speed. In cognitive cryptography, is used for secret communications by making use of random key between source and destination systems. After studying both the techniques a hybrid technique is proposed which incoprated the advantages of both the techniques.

Raju et al. [4] discuss about how the cloud computing has become an important part in majority of application areas like government, business and commercial sectors. Although biometics and cloud computing make a perfect combination in the field of security. The revolution of cloud has posed a security threat on biometric templates, which has become a matter of matter of concern now. Many researchers are working upon the Biomertic security but a foolproof technique has not been suggested till date. He elaborates various security problems like loss of trust, multi tenancy and loss of control. This paper presents a theoretical approach using Forward Error Correction.This approach helps in correcting the errors during transmission.

Das et al. [5] stated that among all the other types of authentication methods, biometric authentication is most widely accepted. Authors specifically stressed upon the need of remote and on demand authentication system for the environment where the objects are subjected to movement like soldiers in battlefield. They suggested that if fingerprint based authentication systems are combined with the traditional ones then secutity would reach to a next level. This paper proposes an optimized and energy efficient solution for in-field fingerprint-based authentication. Authors elaborated the concepr of Human Body Communication for on-body data transfer. In the process to accomplish the above stated objective, they made use of **custom-**built hardware prototype using COTS components. The authetication was crucial to detect any insider threat. The various phases of in-field fingerprint authetication system are of biometric sensing, data compression, encryption and communication. The possibilities for resource allocation in in-field authentication system involve selection of wearable fingerprint sensor, choice of algorithm and selection of on-body communication technique.

Alzahrani, [6] emphasised upon vaulted verification technique. In this technique, the fingerprint sample is divided into a triangle structure in order to improve the accuracy of template. The triangle is made from three minutiae points. Thereafter the triangles are divided into blocks. Each block is then encrypted seperately. The blocks are then swapped with a random bitstring. At the time of identity verification, destination system creates a new triangle which is matched against each block to recover the bit string.

Author also suggests a scheme based on merkle hash tree for the purpose of user authetication. According to this technique, the fingerprint sample is not sent on the cloud rather a signature is generated form the hash values of fingerprint sample. This technique, the misuse of data can be avoided to a very large extent with optimum computation cost.

III. PROPOSED METHOD

As the technology is drifting towards remote authentication, a number of techniques have already emerged. After analysing and understanding various techniques of encryption, another technique has been proposed which is discussed below.

A. Software Specifications

It has been observed that for processing of any fingerprint image an application tool would be required. So the Matlab R2009 was procured and installed with its complete tool box and modules.

B. Procedure

Before actually encrypting the fingerprint sample there is need to pre-process it. The pre-processing of fingerprint is done in following phases:

- Loading of image
- Image Enhancement
- Cropping
- Binarization
- Image Thinning
- Minutiae Marking and Extraction

I Loading Fingerprint image. The fingerprint images are extracted from sensor and saved in database from which any random sample is selected for processing. The fingerprint template loaded in the software is shown in figure 1.

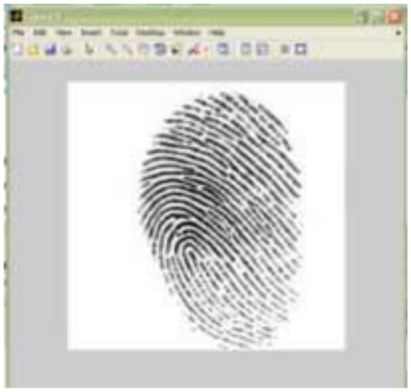


Fig.1

II Image Enhancement. Before, we actually start with the process the fingerprint sample undergoes a process of Image Enhancement in which the image is made clearer for smooth functioning of further operations. This process includes judging the quality of sensor, enhancing the contrast between ridges and valleys and connecting light and almost disappeared lines. Enhanced image is shown in Fig 2.

III CROPPING: It has been studied that the minutiae points present on the corners and boundaries of the sample are not the significant points and should not be considered for processing. These insignificant points are also called as spurious minutiae points. So the image was cropped and insignificant points were supposed to be removed. The image after being cropped looks like as shown in Fig 2.

Now here this image spurious minutiae points has been eliminated which further reduced the number of points and also reduced the processing time.

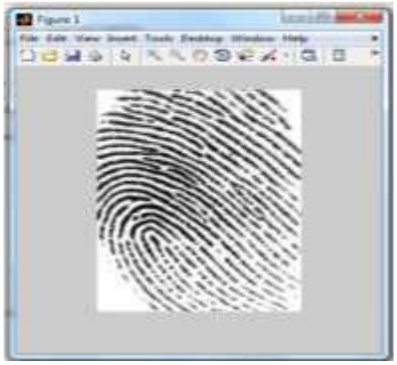


Fig.2

IV Fingerprint Image Binarization. In this method, the sample fingerprint image is divided into certain blocks, say (16X16). The intensity value of these blocks is analyzed and accordingly the pixel value is marked as 1 if intensity value of that pixel is greater than mean intensity of that block and 0 otherwise. Shown in figure 3.

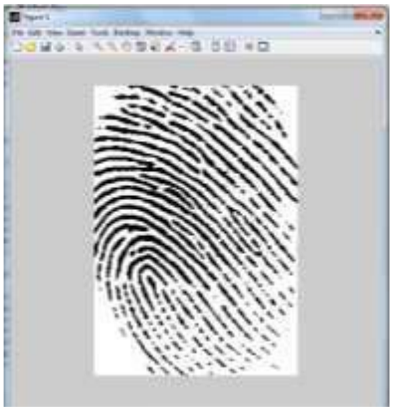


Fig.3

V Fingerprint Ridge Thinning. As the name suggest, this is the process of thinning in which thickness of each line is reduced to a single line. The image is reduced to the level where no further removal of pixels is possible. Shown in figure 4.

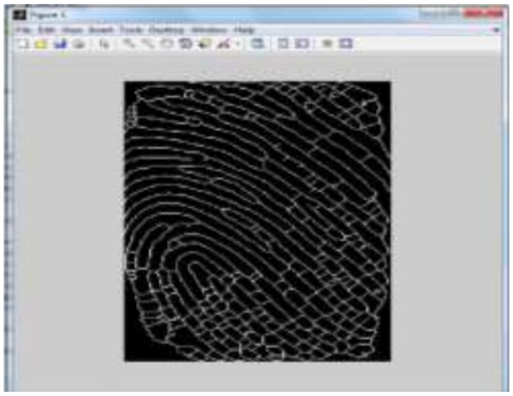


Fig.4

VI Minutia Marking. In this step all the minutiae points are marked.

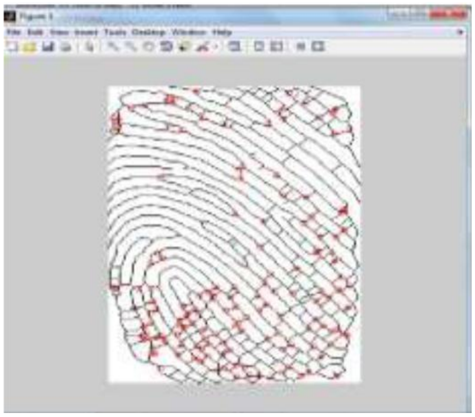


Fig.5

VII Encryption: Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge that allows them to change the information back to its original, readable form.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to.

To encrypt a fingerprint, here minutiae points are represented in the form of (x,y) coordinates. The prerequisite before implementing the alogorithm is that the image has been preprocessed. Following algorithm has been suggested for securing a Fingerprint sample:

1: Extract all minutiae points in terms of (x,y) Coordinates i.e. $\{x_1y_1,x_2y_2,x_3y_3\ldots x_ny_n\}$ as shown in Fig 6.

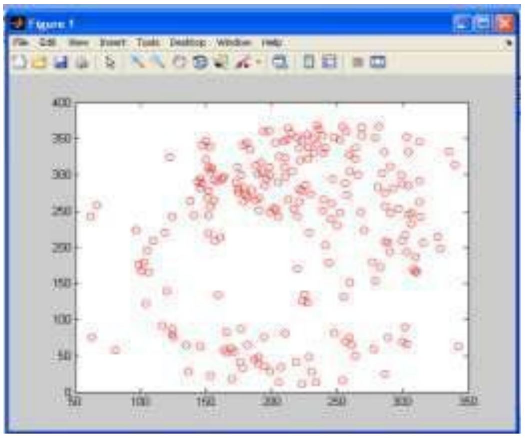


Fig.6

Thereafter, the points were seperated into two different arrays as shown in Fig 7.

$X=\{x_0,x_1,x_2\ldots x_{n-1}\}$

$Y=\{ y_0,y_1,y_2\ldots y_{n-1}\}$

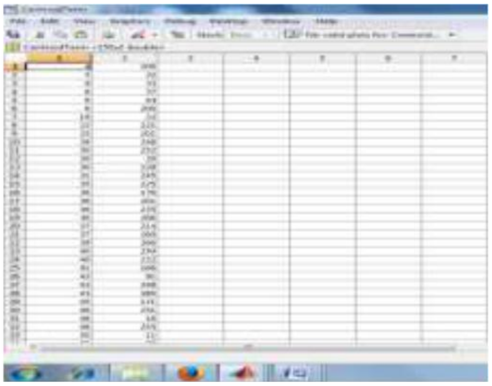


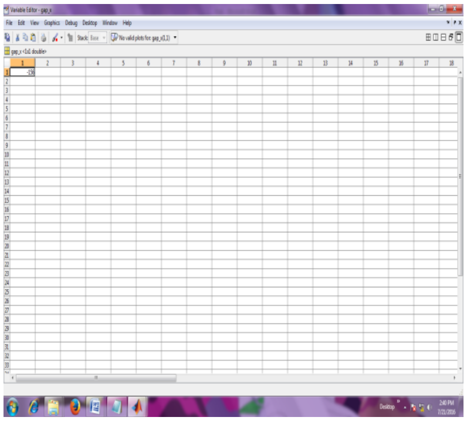
Fig.7

2: All the points from both the arrays are swapped.

$Xs=\{y_0,y_1,y_2\ldots y_{n-1}\}$

$Ys=\{ x_0,x_1,x_2\ldots x_{n-1}\}$

3: From these swapped arrays which constitutes of minutiae points, the first and last element of both the is extracted. After subtracting first element from the last one, the difference is calculated. These values are known by name of x_d for x and y_d for y.


Variable Editor - gap_x
File Edit View Graphics Debug Desktop Window Help
Stack: Base
No valid plots for: gap_x(1,1)
gap_x <1x1 double>
Desktop

gap_x <1x1 double>

	1
1	-156

Fig.8

4: The value obtained in above step is subtracted form all the elements of array.

$Xm=\{y_{0\text{-}yd},y_{1\text{-}yd},y_{2\text{-}yd} \ldots y_{n\text{-}1\text{-}yd}\}$

$Ym=\{ x_{0\text{-}xd},x_{1\text{-}xd},x_{2\text{-}xd} \ldots x_{n\text{-}1\text{-}xd}\}$

5: After this step, the median of both the arrays is calculated namely x_i and $y_{i.}$

6: All the array elements are then divided by y_d and x_d respectively.

$X_f=\{y_{(0\text{-}yd)/yi},y_{(1\text{-}yd)/yi},y_{(2\text{-}yd)/yi} \ldots y_{(n\text{-}1\text{-}yd)/yi}\}$

$Y_f=\{ x_{(0\text{-}xd)/xi},x_{(1\text{-}xd)/xi},x_{(2\text{-}xd)/xi} \ldots x_{(n\text{-}1\text{-}xd)/xi}\}$

On the basis of all the mathematical calculations done above, a key is secret generated. This key is sent along with data on the cloud. Whenever the sample is required to be downloaded, it is decrypted with the help of this key.

Key 1 = (x_{irev}, x_{n-1}-x_d, n-1)

Where

x_{irev} : is the reverse of median calculated form x coordinates.

x_{n-1}-x_d = total number of elements-difference calculated.

n-1: number of elements in x array

Key 2 =(y_{irev}, y_{n-1}-y_d, n-1)

y_{irev} : is the reverse of median calculated form y coordinates.

y_{n-1}-y_d : total number of elements-difference calculated.

n-1: number of elements in y array

IV. CONCLUSION

The processing of fingerprint is a tedious task. It is very important to get the samples of good quality so that further processing could be applied on it.

Image quality is related directly to the ultimate performance of automatic fingerprint authentication systems. Good quality fingerprint images need only minor preprocessing and enhancement for accurate feature detection algorithm.

Further, more emphasis has been laid on defining the local criteria, in order to establish the validity of a minutia point, which is particularly useful during fingerprint matching and adopting more sophisticated identification models, for instance extending minutiae definition by including trifurcations, islands, bridges, spurs etc.

The finger print sample has been loaded and cropped to avoid spurious minutiae points. The sample has also undergone binarization and thinning. The minutiae extraction algorithm extracted all the minutiae points which were encrypted so that any unauthorized person could not be able to tamper the sample.

At the senders end, encryption algorithm is provide to encrypt the exact location of minutiae points, after which the sample can safely be transferred anywhere.

At the receivers end i.e. the cloud, decryption algorithm is provided to decrypt the original minutiae points which can be plotted and original fingerprint could be generated.

As the field of biometrics is in is growing state and that too very fast, this technique can be implemented with cloud computing where the people will get opportunity to authorize a large number of transactions like storing data, manipulating data and accessing data on the cloud even from remote locations.

Security is fundamental to the success of using cloud-based applications for your business. When you adopt biometrics for your cloud computing you will experience reliability, scalability, cost savings, and several other benefits. This is why biometrics are the wave of the future for cloud computing.

References

1. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar (2008). Biometric Template Security, EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics.

2. Anil K. Jain Arun Ross Umut Uludag. Biometric template security: challenges and solutions, Michigan State University West Virginia University Michigan State University.

3. Mehreen Ansar, Muhammad Sheraz Arshad Malik, Mubeen Fatima, Sadaf Aslam,
Anum Rasheed, Iqra Nazir (2018). Biometric Encryption in Cloud Computing: A Systematic Review,IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.8.

4. S.Viswanadha Raju, P.Vidyasree, G.Madhavi (2014). Enhancing Security Of Stored Biometric Template In Cloud Computing Using FEC, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-2.

5. Debayan Das, Shovan Maity, Baibhab Chatterjee & Shreyas Sen.In-field Remote Fingerprint Authentication using Human Body Communication and On-Hub Analytics, School of Electrical and Computer Engineering, Purdue University, USA.

6. Hamdan Ahmed Alzahrani (2006). Remote Authentication Using Vaulted Fingerprint Verification, The University of Sydney, Australia.

7. Ann Cavoukian, Ontario (2008). Biometric Encryption: A tranformative technology that delivers strong security and privacy. Institue of electrical and electronics engineers.

8. Juan M. Vilardy.et.al (2008). Fingerprint Encryption using Fractional Fourier Transform. 5th. European Congress on Computational Methods in Applied Sciences and Engineering.

9. Anthony.et.al (2009). Securing Biometric Data. Seminar Biometric & Security. Mitsubishi Electronic Research Laboratories.

10. Jain, A., Nandakumar, K. and Nagar, A (2013). “Fingerprint Template Protection: From Theory to Practice,” Security and Privacy in Biometrics. Springer London, 187-214.

11. J. Bonneau et al (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, IEEE Symposium on Security and Privacy, pp. 553–567.

12. A. Jain, K. Nandakumar and A. Nagar, (2008). Biometric TemPlate Security, EURASIP Journal on Advances in Signal Processing, Vol. 2008, 2008, pp. 1-17.

13. N. Ratha, J. Connell and R. Bolle (2001), “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” IBM Systems Journal, Vol. 40, No. 3, 2001, pp. 614-634.

14. Murugan, C. A., & KarthigaiKumar, P. (2018). Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms. Mobile Networks and Applications, 1-6.

15. Gawade, S., Bharti, A., Raj, A., & Madane, S. (2017). Biometric Authentication using Software as a Service in Cloud Computing. International Journal Of Engineering And Computer Science, 6(3).

16. Chand, K. S., & Rani, B. K. (2018). Biometric Authentication using SaaS in Cloud Computing.

17. Bala, Y., & Malik, A. (2018). Biometric Inspired Homomorphic Encryption Algorithm for Secured Cloud Computing. In Nature Inspired Computing (pp. 13-21). Springer, Singapore.

18. A. K. Jain and U. Uludag (2003). “Hiding biometric data,”IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 25,no. 11, pp. 1493–1498, 2003.