International Journal of Engineering & Technology, 7 (2.32) (2018) 307-311

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Survey on Using Biometrics for Cloud Security

K.Ruth Ramya[1], D.N.V.Saikrishna[2], T.Sravya Nandini[3], R.Tanmai Gayatri [4]

[1,2,3,4]Dept of CSE , K L E F,Vaddeswaram, India
**Corresponding author E-mail: ramya_cse@kluniversity.in*

Abstract

Cloud computing the most emerging data storage and processing technology. Today many organizations are using cloud-based data storage because of their complex data management. Even though cloud is attracting many users towards using it but there is a requirement of security concerns to be taken care of because cloud is untrusted, the data which individual stores on cloud will be transparent to cloud administrator also which may be confidential. So, while using cloud security is the primary concern. In this paper, we proposed a scheme to encrypt cloud data using user attribute-based encryption. Which is a public key crypto technique in which key will be based on the attributes of user. The attributes we used are biometrics of user who is going to upload the data.

Keywords:*Biometrics, Cloud data encryption, Finger print, Cloud security, Attribute-based encryption..*

1. Introduction

These days computation over cloud has become most common for all type of applications. As the storage on local disks is not too reliable, cloud storage is attracting every individual to store data on cloud which can be accessible across the globe. The number of users increases, the security level need to be upgraded which means data over the cloud may not be secured because when particular data is transferred to the cloud the data is transparent to two parties. One who is using cloud services and the cloud administrator. While dealing with the data security aspect we can't trust any single individual, Cloud admin may be the victim to steal the data. So, while storing data over the cloud it need to be encrypted and stored on the cloud, so that no one except the owner will know the actual raw data. Even the cloud administrator cannot access the data without knowing encryption mechanism. So, now data is said to be secured to some extent but not totally we can trust these encryption mechanisms to avoid that there is another method of encryption mechanism which is user attribute-based encryption mechanism which uses the attributes of user in order to generate key which is used to encrypt the data. Now some more confidentiality is added to previous mechanisms because the attributes will be known to the user only. But, those attributes will be stored somewhere in the cloud only where the actual encryption process is happening. Which means the user attributes will be transparent to the cloud administrator also. So, in providing security the strength of encryption mechanism will not depend on the algorithm used but it depends on the strength of the key used here key (user attributes) is transparent. Therefore, how much complex the algorithm may be, cracking that algorithm will be easy thing once cipher key is known. So, including attributes of user in generation of cipher key is a good thing but storing/mentioning those during key generation on the cloud is safe to some extent only. To increase trust for the cloud users those attributes the of the user is considered but not the text or any other but the BIOMETRICS of the user who is going to store data is used to generate cipher key which is used in encryption and decryption process [1].

2. Biometrics:

These are the forensic techniques which uses the physical characteristics of individual like finger prints, hand geometry, iris, voice, face in order to authenticate him/her to access a particular sensitive data. The suitable biometrics are used based on the type of application or based on necessity of level of security. The biometric data inputs are seized or captured using various biometric devices such as finger prints, iris, face etc. These biometric devices are classified into two groups discrete devices and non-segregated or integrated devices. Discrete biometric devices concern to the category of fingerprint, iris that requires connectivity to a network host or host device such as PC, laptop, etc. Integrated biometric devices have a sensor which are integrated into device package.

2.1. Finger Prints:

Finger prints of users are used as attributes for security over long period of time but not too much extent they are used for more confidential systems only like in banking sector administrators will use their finger print in order to unlock the database access. Finger print scanners are affordable and are flexible to be used over many computer applications [2]. The sample image of finger print is shown in fig 2.1.



Fig 2.1. Finger Prints sample

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Advantages of finger prints include Reliability is very high in finger print recognition. This requires very less space for storage in order to store biometric template, reduction of database size must be required. Finger prints are systematized. It is very easy to use. They will have some disadvantages too; Finger print recognition is unwanted to some people because it is related to criminal recognition. Compression of image is required in this factor. Recognition of the finger print is very difficult when the fingers skin is very dry and dirty. Recognition of children's finger print is not significant because the size of their finger print size changes so fast.

2.2. Hand Geometry:

The Hand geometry-based authentication system is based on a measurement taken from the palm of user such as length of palm vein, size of palm, length and width of fingers etc. Viable hand geometry devices are manufactured since 1980s, hand geometry is the first biometric to widespread computerized use. Scanning palm print with high accuracy is needed because palm geometry may match between two individuals [10]. Scanning the palm of users has to be done periodically in order to avoid conflicts. Because the palm length, length and width of fingers are considered they will grow with age of person so, this was not that much popular as fingerprint scanners [3]. Hand geometry is very reliable when compared with other types of identifications. For comparison it uses palm vein pattern as shown in fig 2.2.

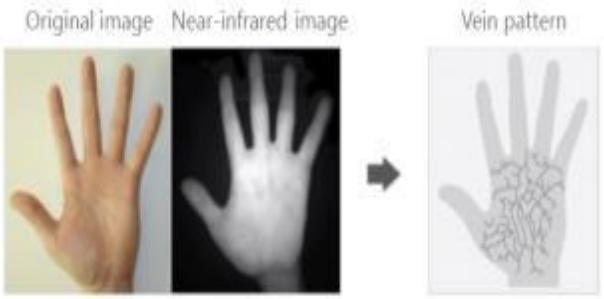


Fig 2.2. Palm Recognition

Advantages of Hand geometry *are* the data of hand geometry is easy to collect, a good frictional skin is required by image systems and special lighting of retinal data is required unlike the other finger prints. It is very simple, easy to use and affordable. Environmental problems such as dry which causes dry skin is not a big issue. Usually considered less prominent than fingerprints, retinal, etc. *Disadvantages are* hand geometry is not distinctive and they cannot be used in identification of systems. In hand geometry biometrics the size of data is very large and it is not absolute to use it in embedded systems. Not consummate for growing children.

2.3. Iris Recognition:

Iris scanners depends on the nerve endings inside eyes they will scan and mark the nerve endings in the eyes of user and store those points and those stored points will be used further to authenticate the user to access sensitive data. This system failed in some cases like while there is any sensation in the eye of user and eyes become reddish in that case iris recognition system fails to authenticate person. This is not much popular for authentication purpose, but it is used for some confidential issues. It is used by hundred million persons in many countries all over the world for expedience purposes such as passport free automated border crossings and many national ID programs. Mostly it is extreme defiance to false matches. Methodology is shown in fig 2.3.

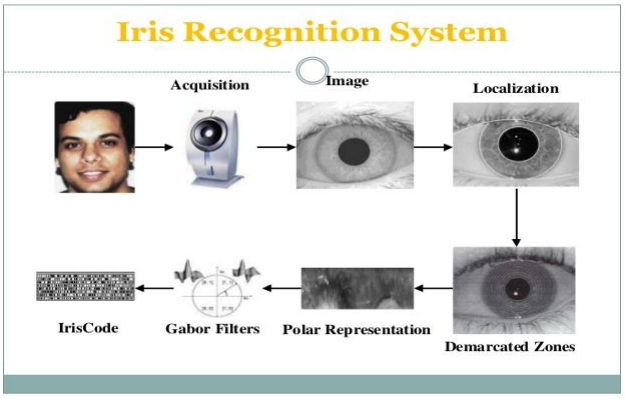


Fig 2.3. Iris Recognition System

Advantages include high accuracy. Time for verification is less than 5 seconds only. The iris of a dead person would degenerate too fast, so we may not need any extra precautions to be taken by retinal scans and we must me sure that user is a living human being. *Disadvantages are* Large amount of memory is required to store the data. Iris recognition is very expensive when compared with other techniques. It is very inquisitive.

2.4. Voice Recognition:

Voice recognition system is one of the biometric authentication system which uses vocal tone of the user to identify whether the correct person is accessing the data. Once the vocal tone of user saying particular words will be stored and while authenticating the user need to speak out those words with same. voice if voice matches then authentication system will unlock the security provided for that data. As shown in fig 2.4 voice wavelets will be compared.



Fig 2.4. Voice Recognition.

Advantages are Non-invasive and highly socially acceptable. Time for verification is upto 5 seconds. The technology which is used in voice recognition is very cheap. Disadvantages include A person's voice is changes due to the occurrence of illnesses like cold and cough, this causes identification of persons voice very difficult and hard to recognize. An individual's voice can be recorded easily and also be misused for unauthorized access of PC or any other network. Very less accurate.

2.5. Face Recognition:

Face recognition system scans the users face and predict the features of face like eyebrows, lips, eyes etc. and store them in database during authentication same features which are stored will be extracted again from users face and matched with the previously stored values and unlocks if matched[4] .

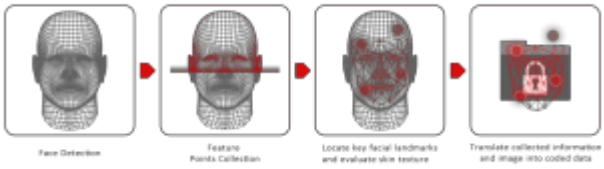


Fig 2.5. Face recognition.

Advantages are Face recognition does not require any physical commerce from the user. In face recognition we recognize the face by submissive identification. It is inexpensive identification technique and friendly. Disadvantages are It cannot identify the difference between two identical replica or twins. Face cannot be recognized when people shave shave their beard or grow their beard, false recognition of face is done when they change their hair style.

2.6. Signature Recognition*:*

Signature recognition is visual or behavioral biometric. We authenticate the individual by analyzing his handwriting style in his particular signature. Signature recognizing systems contains sensors such as touch sensitive writing surface, pen etc. These sensors detect the direction, pressure and angle of the writing. The system converts the writing into a graph and identifies whenever the signature is changed during authentication. This Signature recognition is of two ways which is static and dynamic. In static recognition when we write the signature on paper, it is digitized through a scanner or camera, the biometric authentication system identifies the signature by examining its shape. This is known as "offline". In dynamic recognition we write the signature or a smart phone or a tablet. This is known as "online". Signature timing is noted in dynamic recognition. We can forger the signature into duplicate, but it is not possible to duplicate the timing of the signature, the timing changes according to the pressure x, y. It uses edges of lines as starting points to recognize signature as shown in fig 2.5 (1,2,3).

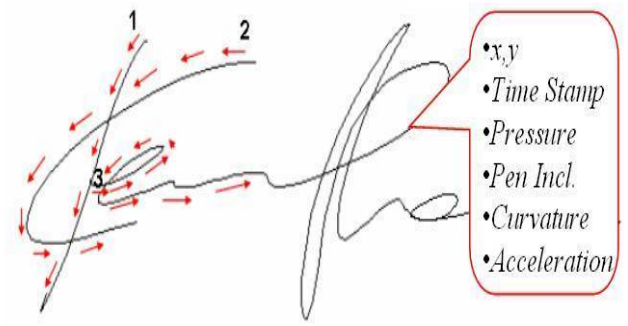


Fig 2.6. Signature Recognition

Advantages includes Verification time is very less in signature recognition. We use very cheap technology. We mostly use this in industrial purposes. Disadvantages include It is used to verify the subjects which are based upon their unique signature and individuals who did not sign their names in uniform manner may cause problems in verifying their signature. Error rate of signature recognition is 2 in 100.

The Biometric Recognition Systems are used to identify the person based on the feature vectors of any one of the biometric that the person possesses. Among all the biometric recognition systems finger print has gained its importance and is successfully implemented in numerous real- world applications because everyone is known to have a unique finger print which are immutable throughout his/her life irrespective of their ages. So, finger prints are widely used in authentication systems as it will ensure high security. There are many applications where biometrics are used as key for authenticating users for better security. Biometrics are used as authentication systems such as on demand biometrics for cross authentication systems for faster access while logging into user accounts without using usernames and passwords [6].Biometrics are used for systems where complex passwords are needed because those complex passwords are difficult to remember [7]. In major security problems like security in ATM machines can be replaced with biometrics [8]. These days biometrics are made as authentication for android smart phones future all the android applications will replace passwords with finger prints in order to login to particular application finger print is enough no need of remembering usernames and passwords which are difficult to remember and may be predictable. Android security using biometrics are implemented using facial recognition authentication system for African cashew farmers who need to carry out their transactions through mobile security need to be high because huge amount needed to be transferred between them [9].

3. Cloud:

It's nothing but remote computing or a remote computational system which can store, manipulate the data. Most of the users use user id or username and password for authentication purpose but the main issue with this approach 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 biggest issue in cloud computing is the cloud contributor can also access the data of the authorized user. Security problem is very major component in cloud computing. Whenever we are using a local system for all our needs if that system crashes there will be no alternative for us to get back our data so, these days people are moving towards cloud for data storage where the data can be stored on multiple data servers if one server crashes the data will be safe in other server. 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.

3.1. Cloud Based Biometric Technologies:

Recently, Cloud ABIS™ is introduced which is highly ascendible, cloud based biometric matching system. This cloud based biometric matching system is built over 15 years of experience in large scale biometric technologies. This comparing system reinforce fingerprint, finger vein, face and iris recognition. This cloud based biometric matching system which is also known as CloudABIS™ can contrast lakhs of fingerprint templates at a time per second but we need an internet connection from the client to influence the power and accessibility of our cloud biometric platform. CloudScanr™ can work immediately across any kind of browser.

3.1.1. Emerging Market Trend on Cloud Based Biometrics:

There are many surveys conducted on cloud based biometric system, the survey name Bloomberg survey has stated that by 2020 the biometric based cloud computing will earn up to 270 billion dollars mainly due to its pliability, movability and savings of cost. The cloud users are increasing day by day and recently the cloud-based platforms are provided or made accessible to the mobile applications also. According to recent studies, more than 240 million users of businesses uses cloud based biometric authentication system via mobile devices by 2015.This has raised the revenue of biometric based cloud computing by 5.2 billion dollars. Some smart phone manufacturing companies like Samsung which has released licenses to SRI's iris solution of mobiles and then they introduced Samsung Galaxy Tab Pro 8.4 tablet for biometric based authentication and some other companies like HTC, Apple and Sony has already instigated some biometric features such as fingerprint, voice, face recognition to their products. These features are very convenient to the users in securing their cloud data. As new biometric technologies are arriving into the market it becomes very easy to embrace biometric security on cloud.

3.2. Securing Cloud Data Using Fingerprint Authentication Mechanism:

We use fingerprint authentication technique in order to secure cloud data. We use the help of camera of the mobile phone to capture the input finger print image. After obtaining the fingerprint image, we need to extricate the ridge structure from the fingerprint. By this process, the image will be almost identical to the fingerprint image from the fingerprint sensor. The user can use his fingerprint to login each and every time when he tries to access the cloud.

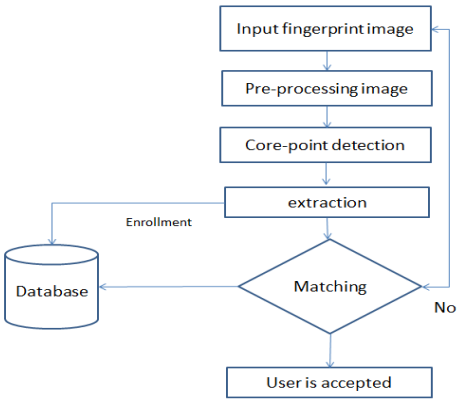


Fig 3.2.1. Securing data on cloud

As shown in fig 3.2.1 first phase in which input fingerprint image is given is call as enrollment phase. In this phase, the sensor captures the fingertip of the user. Pre-processing of the image is done to extract the features from the fingertip which is displayed or presented by the user and further it is used to compare the identification or verification of the user. The user needs to provide his fingerprint to the fingerprint sensor whenever he tries to login or access into the cloud-based applications. The user is able to login if and only if when the fingerprint features matches with the features which are stored in the database during the first phase which is enrollment phase. The user is granted to access or accepted only when the features are matched otherwise the user is rejected to access the cloud-based applications. Matching between the user's fingerprint features and the features which are stored in the cloud database is shown below.

3.3. Matching the Features:

Let, S be the similarity.
If S has a low value, it implies there is little similarity.
If S has high value, it implies there is high similarity.
Let T be the Threshold and it is contrasted with the Similarity score which is S.

if (S>T) then
The user is accepted
else if(S<T) then
The user is rejected.

Thus, the biometric authentication system plays a major role whenever the user tries to access the cloud-based application. After the successful access of the user or authentication of the user, the user is directed to the authentic cloud service platform and the user is provided the command to access.

3.4. Risks in Cloud Environment:

As the data is stored remotely the first risk to be considered is security for the stored data. Basically, data that is stored on cloud will not be exposed to anyone, but it is transparent to two parties one is the person who is going to store the data and the other is the cloud administrator. While security is taken into concern no one has to be trusted cloud admin may steal the data. So, for that we need the administrator not to steal data at any concern so during uploading the data into cloud the data needed to be encrypted and stored so that the cloud administrator will not understand what the data is for that there are many encryption mechanisms we can follow to encrypt the data and send to cloud for storage. But for computation on the cloud we need to get back the data again to our local system and perform computation and again need to store the data again on the cloud which is little complex task to be accomplished so everyone who uses cloud will make computation on cloud itself and while performing computation on the cloud our conventional approach of encrypting and storing won't work because the data on the cloud is not the raw data and the decryption process will not be known to cloud so then the process of encryption and decryption has to be done on the cloud only for that we need to perform/store that encryption process on the cloud only.

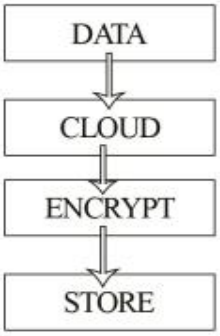


Fig 3.4.1. Encrypting and storing data on cloud

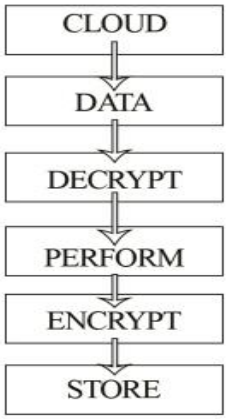


Fig 3.4.2. Performing computation on cloud

In the above figure 3.4.1 & 3.4.2 the data will be stored raw data will be sent to cloud and there the encryption mechanism takes place and stored while performing any operations over cloud the data will be decrypted and used for computation and again after computation the encrypted and that data will be stored. In case of encrypting on local machine and storing on cloud is more burden because each time we need to perform computation only on local machine few computations like data analytics are very difficult to perform in local system. So, this method fails in those cases. In case of performing encryption and decryption process on the cloud the raw data and the encryption mechanism needed to be transferred to cloud. Therefore, the encryption mechanism and will be on the cloud and will be known to the administrator. As the encryption algorithm is known to the third party which means we are taking more risk on data. To avoid these, we need to use better encryption techniques. Encryption mechanism's strength will blindly depend on the strength of cipher key used for encryption as the strength of key is more it is not that easy to predict the key and the data will be safe so the key generation is the major task in encryption. Later key generation is made complex by involving user

attributes in the key generation process which means while generating the cipher key the user attributes like name, DoB, email, phone number etc. are used and key is generated based on key generation algorithm. Drawback with this mechanism is the attributes will be known to the administrator because they are stored on cloud itself so later moved on to next level of using user attributes in key generation. Biometrics are involved in key generation process which means biometric properties of particular user will be used and the key will be generated based on an algorithm of their choice.

4. Key Generation:

4.1. Using Palm Vein in Key Generation Process:

As mentioned in figure 4.1.1 the process will be carried out and hand geometry of user is used for key generation purpose. From the palm vein, particular minutiae points will be extracted and those set of points will be used for key generation purpose [5].

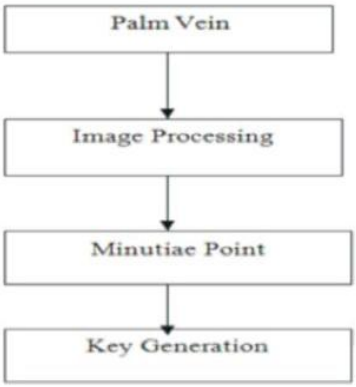


Fig 4.1.1. Feature extraction in palm vein

4.2. Key Generation Using Finger Prints of User:

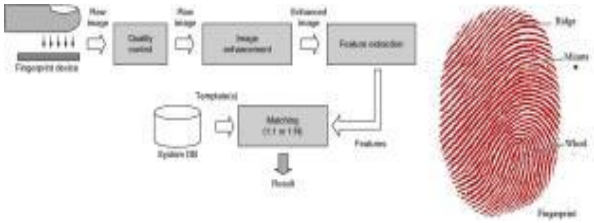


Fig 4.2. Fingerprint extraction and authentication

As shown in fig 4.1 Finger prints of user needed to be scanned using a mechanical scanning device and check for quality if the quality is enough for image processing then send it for image enhancement where the original image will be modified and an image which is optimal for feature extraction will be generated and from that enhanced image the feature extraction is carried out based on our requirements. Considering minutiae points and using them to extract points and store them to use is one approach but storing them may lead to security issues in some cases. So, storage of extracted points is not safe. Because the application is not only matching the data and providing authentication, but encryption and encryption process also depends on those points only.

5. Cloud Data Encryption Technique:

Cloud is most preferable when there is a large amount of data(big data) which is used for analytics applications so encrypting that large data at a time is quite complex issue, That total data will be divided into small parts and those sub parts of data will be sent for encryption and that are stored on cloud which means we are splitting cloud and encrypting then when there is retrieval of data those particular portions of data will be decrypted and combined to form the actual data and necessary calculations will be performed on that data [5].

6. Algorithm:

1. Authenticate user for accessing.
2. If ok Scan the finger prints using finger print scanner.
3. Extract the features from scanned print.
4. Using those features generate the cipher key.
5. Split the data on the cloud into small parts.
6. Using the previously generated cipher key encrypt the small portions of data and store them in sequence.
7. When the retrieval of data is triggered by cloud again ask for authentication
8. If ok scan finger prints again and generate cipher key.
9. Decrypt the required data using immediately generated cipher key.
10. Combine the small portions of decrypted data to get back raw data.

7. Conclusion

Even after the authentication is done and cloud access is granted the data needed to be decrypted in order to get original data so if the finger prints given is wrong the data decrypted will also goes wrong and raw data will not be exposed to no one except the owner of that data.

References

[1] Iniya Shree, C. Vijesh Joe, K. Narmatha, S. Shinly Swarna Sugi "Providing Biometrics Security for Load Balanced Cloud Data Storage" Middle-East Journal of Scientific Research.
[2] A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification", IEEE Trans. Pattern Anal. Mach. Intel.
[3] Michael Goh Kah Ong, Tee Connie, Andrew Teoh Beng Jin, David Ngo Chek Ling, "A single-sensor hand geometry and palm print verification system", Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, Berkley, Cali-fornia, 2003.
[4] Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D. Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition.
[5] Boneh D., Di G., Ostrovsky R., Persiano G. (2004), "Public key encryption with keyword search", Advances in Cryptology-Euro crypt, Springer, Berlin/Heidelberg, pp 506–522.
[6] Christian Holz, Frank R. Bentley, "On-Demand Biometrics: Fast Cross-Device Authentication", #chi4good, CHI 2016, San Jose, CA, USA.
[7] Mohammed Nasir Uddin, Selina Sharmin, Abu Hasnat Shohel Ahmed and Emrul Hasan, Shahadot Hossain and Muniruzzaman, "A Survey of Biometrics Security System" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10.
[8] Dhiraj Sunehra, "Fingerprint Based Biometric ATM Authentication System", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 11.
[9] Shah Faisal Darwaish, Esmiralda Moradian, Tirdad Rahmani, Martin Knauer, "Biometric identification on android smartphones", Science Direct – Procedia computer science.
[10] Inass SH. Hussein and Md Jan Nordin, "Palm Print verifica-tion using invariant moments based on wavelet transform", Journal of Computer Science.