Biometric Authentication using SaaS in Cloud Computing

[1]K.Sarat Chand, [2]Dr.B.Kezia Rani,
[1]M.Tech Student, [2]Asst.Professor,
[1]Dept.of Computer Science and Engineering,
[1]Adikavi Nannaya University, Rajamahendaravaram, India

Abstract:

Now a day's cloud users are facing the major problem of fake logging in and data theft. So it is required to authenticate the cloud user that requests access to an account for providing privacy and security .Present days cloud computing is becoming a hot trend in IT industries. Most of the enterprises are using cloud for storing and maintaining their huge data on cloud servers. In olden day's security is given by passwords and pins. So Hackers are able to crack these passwords, so the data is not secure until we have a secure mechanism to protect the data from intruders and hackers. So we are using the concept of Biometric Authentication along with data compression and data encryption. The techniques of biometric authentication in cloud face performance issues like time and space complexities. For the security purposes advanced encryption algorithm is used. In recent years, biometrics and computer technology have joined together in order to improve the security in everyday activities such as access control, cash terminals, public transport, internet, smart card readers. With biometric based security systems there is no longer any one need to remember a large number of PIN'S and Passwords, so the genuine biometric characteristics of every individual play the role of personal identity code in front of the world. This paper proposes to improve the security of generating the biometric key from fingerprint biometrics with its feature extraction using AMBA algorithm. The secret value is encrypted with biometric key using symmetric Advanced Encryption Standard (AES) Algorithm

Key words: Biometric Authentication, Finger Recognition, Cloud Authentication, Data protection, Data Encryption, AES (Advanced Encryption standard)

I. INTRODUCTION Today cloud computing is becoming a humans daily life activities. Most of the enterprises are using cloud for storing and maintaining their huge data on cloud servers. But security of critical data over the cloud has become a concern for both cloud service users and providers .In old days people generally use passwords for emails and bank accounts etc. Hackers are able to crack these passwords easily. So, the data is not secure until we have a secure mechanism to protect the data from intruders and hackers. To over comes these Biometric is combined with AES. Biometric system is combination of sensors, feature extraction and matching modules which implements recognition algorithms. Trusted and faithful systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting for their services and corresponding applications. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. The purpose of establishing the identity is to ensure that only a legitimate user, and not anyone else, accesses the rendered services. Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioural characteristic. Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioural characteristic (such as your handwritten signature), or something that is a combination of the two (such as your voice). Biometrics allows us to confirm or establish an individual's identity based on who he/she is, rather than by what he/she possesses as from ID card or what she knows for example password (cryptal or non-cryptal) . In much simpler way Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics. There are many types of biometric technologies on the market: face-recognition, fingerprint recognition, finger geometry, hand geometry, iris recognition, vein recognition, voice and signature. The method of biometric identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: The person to be identified is required to be physically present at the point-of-identification or the identification based on biometric techniques obviates the need to remember a password or carry a token or a smartcard. With the rapid increase in use of PINs and passwords occurring as a result of the information technology revolution, it is necessary to restrict access to sensitive/personal data. By replacing PINs and passwords, biometric techniques are more convenient in relation to the user and can potentially prevent unauthorized access to or fraudulent use of ATMs, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports, driver's licenses and insurance cards may be forgotten, stolen, or lost. Various types of biometric systems are being used for real-time identification; the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan, speech, face, and hand geometry. During matching, the query biometric sample is matched with the reference information which is stored in the database to establish the identity associated with the query. The operation is done in two stages **:**

1. Enrolment
2. Identification

II. Enrolment:

In this stage the biometric information of the person is stored in the database. The implementing in enrolment to match finger print data of user for authentication in cloud. Stored the users fingerprint data in compressed form on a cloud database for the time and use that for matching whenever a user tries to login the next time.

III. Identification:

Biometric scanner to extract fingerprint of user. Finger print data will be transmitted in the compressed from for security of user biometric data. There is a matching module to match the fingerprints against the one stored on the database. If the finger print matches, it will allow the registered user to login.

IV. Why Biometrics?

Biometric is derived from Greek word, based on two words,"bio" meaning **life** and "metric" meaning **measure.**

Biometrics is a powerful and unique tool based on the physiological and behavioural characteristics of the human beings. Biometrics is defined as the measure of human body characteristics. It is a technology used to identify, analyze, and measure of individual's physical and behavioural characteristic. Biometric is used for authenticating and authorizing a person. The biometric system uses various filtering algorithms and noise reduction techniques such as median filtering, adaptive filtering, and statistical histogram wavelet transformation. Fingerprint, Finger Knuckle Print (FKP), Eye, Retina, Voice pattern, Iris and Hand measurement. Most physiological characteristics used for security application are fingerprint, iris, face and palm print. Apart from physiological characteristics, behavioural characters like voice, signature and gait moments are also used to recognize the user. During the process of biometric authentication, the systems need to identify whether candidate biometric readings from users match the records in the entity's biometric database.

For example: Biometrics is used regularly by those in fields of forensics, government, transportation, health-care, financial, security, public justice and safety, education, and driver's licenses. Two major obstacles to the adoption of biometrics are the lack of accuracy of some biometric systems and preserving the privacy of individuals' biometrics data.

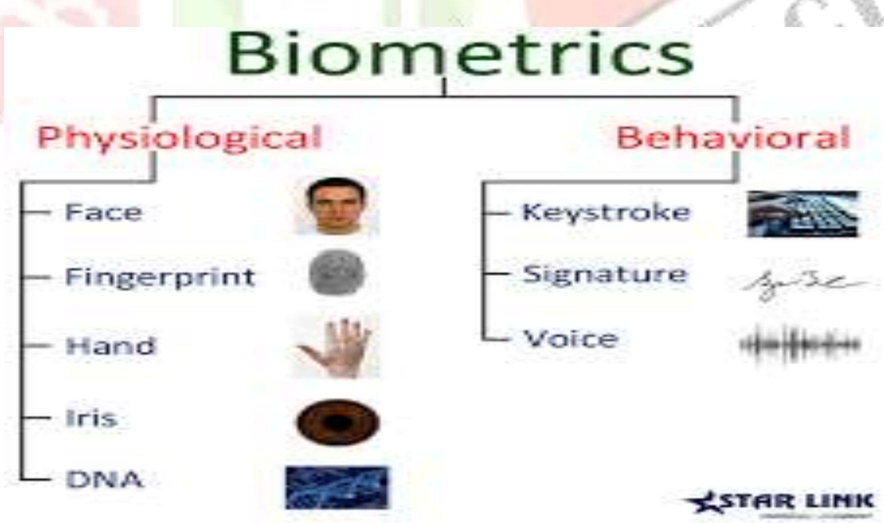

fig 1: Types of Biometrics

History

Sir Francis Galton, in 1892, developed a classification system for fingerprints using minutiae characteristics that is being used by researchers and educationalists even today.

During 1896, subsequently, Richard Edward Henry from Scotland Yard developed a method for fingerprinting by using Galton's theory to identify prisoners by their fingerprint impressions. He devised a classification system that allowed thousands of fingerprints to be easily filed, searched and traced. He helped in the first establishment of fingerprint bureau in the same year and his method gained worldwide acceptance for identifying criminals.

The next stage in fingerprint automation occurred at the end of 1994 with the Integrated Automated Fingerprint Identification System (IAFIS) competition. The competition identified and investigated three major challenges: Digital fingerprint acquisition, local ridge characteristic extraction and ridge characteristic pattern matching.

The first Automated Fingerprint Identification System (AFIS) was developed by Palm System in 1993.

V. Literature Survey:

Based on the analysis of some authors worked as follows:

Chandra Shekhar Vorugunti[1] has introduced a new concept of BioAaas to maintain secure authentication. Based on SAAS model of Cloud it provides a light weight and secure authentication mechanism. It contains two steps for authentication. First is Enrolment and is Verification. In Enrolment process the biometric data is converted into a binary form. In verification process same process will be processed when the user logins to the cloud. The matching module matches the features of the stored data and login data.

Kiran Kumar Ket al.[2] have described that there are two properties of fingerprint namely uniqueness and permanence that are used for identification and verification. These properties are judged by minutiae and ridges. They are grey level fingerprint image, thinning, minute extraction, false minute, matching scores, ridges extraction, minutiae and ridge score fused using strength factor

Dasardha Ramaiah K et al. Proposed a novel approach to detect most effective compression technique based on compression ratio and time complexity. They compared few popular lossy data compression technique like Discrete Wavelet Transform (DWT), K_Mean and 3d Spiral JPEG.

Ms.D.Preetha Evangelina et al. Proposed and efficient mechanism for storing photo albums on cloud storage. They gave the idea to reduce the time complexity of photo album compression for cloud storage. They also proposed cluster.

Hu Chun etal. Have proposed a situation where biometric data is kept encrypted in whole process of transmission and matching. It uses two approaches homomorphism encryption and garbled circuit. It provides highly computing Capability.

VI. System Architecture

In general Biometric Authentication scheme consists of two stages:

1) Enrolment process.
2) Identification process.

The user provides biometric information i.e. fingerprint to the biometric sensor, which converts the biometric data into a binary string. The feature extraction converts the binary string into a reduced representation set of features (eliminates a redundancy).The feature vector of a user is stored into a data base of service provider. In Identification when a user tries to log in into the remote cloud server, same steps will be executed. The feature vector is extracted by the feature extractor and submitted to matching module. The matching module intercepts the feature vector stored against user during enrolment process. The matching module executes the Algorithm to check the matching similarity between enrolment and identification feature process for the user trying to log in.

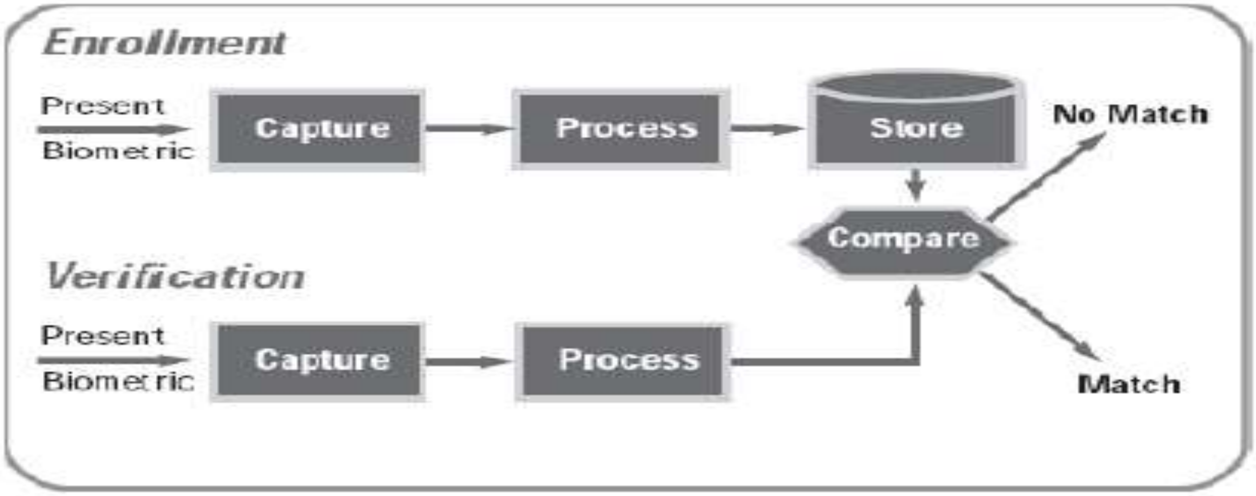

Fig2: Block diagram of Working Biometric system

Whenever the new user wants to access the Cloud the first thing he must do is to register by using his fingerprints. Once he is registered he becomes a valid user and can login to the cloud. The fingerprint image is then stored and encrypted using the Advanced Encryption Standard Algorithm (AES). It is used for security purposes and provides a secret key for the user.

6.1 Back ground work:

AES :(Advanced Encryption Standard)

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and

256 bits respectively. At present the most common key size likely to be used is the

128 bit key. This description of the AES algorithm therefore describes this particular implementation.

Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design Simplicity.

The overall structure of AES can be seen in The input is a single 128 bit block both for decryption and encryption and is known as the **in** matrix. This block is copied into a **state** array which is modified at each stage of the algorithm and then copied to an output matrix both the plaintext and key are depicted as a 128 bit square matrix of bytes. This key is then expanded into an array of key schedule words (The **w** matrix). It must be noted that the ordering of bytes within the **in** matrix is by Column. The same applies to the **w** matrix.

6.2 Inner Workings of a Round:

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage.

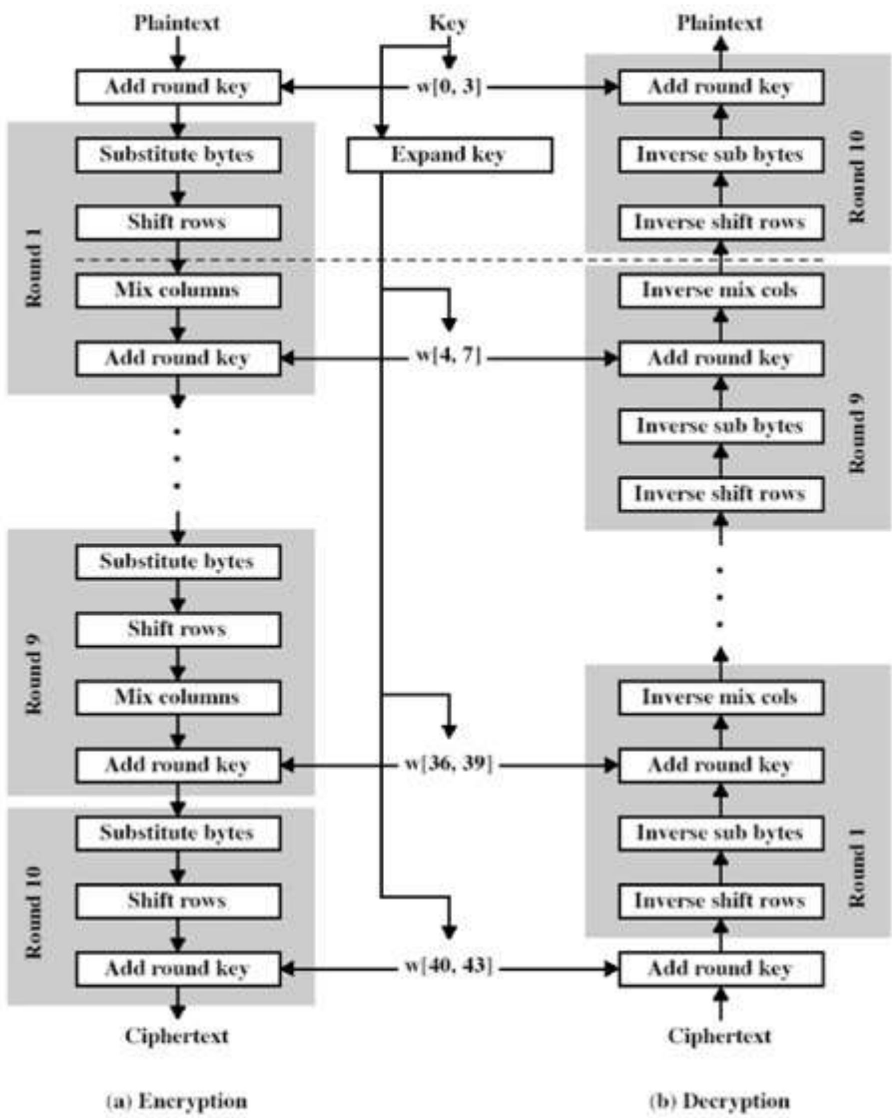

fig 3: Block diagram of AES (Advanced Encryption Standard)

6.3 Normalization:

It is performed to remove the effects of sensor noise and grey level back ground due to finger pressure difference. An input fingerprint image is normalized so that it has a pre-specified mean and variance. Normalization is performed on the segmented fingerprint image ridge structure so as to standardize the level of variations in the image grey-level values. By normalization, the grey-level values are made to fall within certain range that is good enough for improved image contrast and brightness. The first of the tasks of image normalization implemented and adopted for this research is the division of the segmented image into blocks of size S x S. The grey-level value for each pixel is then compared with the average grey level value for the host block. For a pixel belonging to a block of average grey-level value of M, the result of comparison produced a normalized grey-level value.

6.4 IMAGE SEGMENTATION:

There are two regions that describe any fingerprint image; namely the foreground region and the background region. The foreground regions are the regions containing the ridges and valleys. As shown in below fig, the ridges are the raised and dark regions of a fingerprint image while the valleys are the low and white regions between the ridges. The foreground region

.

6.5 Image Binarization/Thinning:

The image obtained from the Gabor filtering stage is binarized and thinned to make it more suitable for feature extraction. The method of image binarization proposed in [10] is employed. The Method sets the threshold (T) for making each cluster in the image as tight as possible, thereby minimizing their overlap. To determine the actual value of T, the following operations are performed on set of presumed threshold values:

a) The pixels are separated into two clusters according to the threshold.

b) The mean of each cluster are determined.

c) The difference between the means is squared.

d) The product of the number of pixels in one cluster and the number in the other is determined. The success of these operations depends on the difference between the means of the clusters. The optimal threshold is the one that maximizes the between-class variance or, conversely, the one that minimizes the within-class variance.

For providing security to cloud, we can use different techniques. Generally passwords are used for authentication. But passwords are easily attackable. This is cheapest as well as simplest technology. So we can use biometric authentication to provide security for cloud computing. Biometric authentication techniques, which are used for securing cloud computing.

The feature extraction is performed on encrypted data. It takes the mean of all the blocks from Advanced Encryption Standard algorithm. This mean is compared with the means of the data that is already stored in the database while registration. This process of matching is done using Advanced Minutiae Base Algorithm (AMBA). It finds the correlation between the two images and gives the result whether he is valid user or not.

VII. Conclusion:

The existing system have technologies that save the whole data on cloud that gives heavy load on the resources which ultimately leads to slow processing. The earlier techniques used for matching images fails in matching those images that have orientation change. So, we proposed a biometric authentication mechanism which allows us to provide secure login cloud server and verifying the user even if the orientation of fingerprint is changed. This is done by an Outsource able two party Privacy preserving Biometric Authentication method. It reduces the threat of data theft and reduces the load on resources

References

[1] Chandra ShekharVorugunti, “A Secure and efficient Biometric Authentication as a service for cloud computing,” IEEE, October 09-11 2014

[2] Kiran Kumar K, K.B Raja, “Hybrid Fingerprint Matching using Block filter and strength factor,” Second International Conference on Computer Engineering and Applications,2010

[3] Dasaradha Ramaiah K and T Venugopal "A novel approach to detect most effective compression Technique Based on Compression Ratio and time complexity with huge data Load for Cloud Migration," IEEE 2016.

[4] Ms D Preetha, Cephas Paul Edward V and Dr. Anandh Kumar P "An Efficient Mechanism for storing Photo Album on Cloud Storage," IEEE 2015.

[5] Hu Chun, Feng Li "Outsource able two party privacy preserving biometric authentication," June 4–6, 2014, Kyoto, **Japan**