Biometric Authentication using SaaS in Cloud Computing

K Sarat Chand[1], Dr. B Kezia Rani[2]

[1]M.Tech Student, University College of Engineering, Adikavi Nannaya University
[2] Asst. Professor, Dept. of Computer Science and Engineering, University College of Engineering, Adikavi Nannaya Univeristy.

---***---

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 Standards 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 Advanced Minutiae Base Algorithm (AMBA). The secret value is encrypted with biometric key using symmetric Advanced Encryption Standard (AES) Algorithm*

Key Words: **Biometric Authentication, Finger Recognition, Cloud Authentication, Data Encryption, Data Protection, AES.**

1. INTRODUCTION

People use passwords constantly, to login to a number of online services every single day. And equally as the number of online services, the person subscribes to Increases, the amount of passwords that person has to call up is more. An average person has to call back about 19 passwords, from online services to local machines [1]. Moreover, the online service providers to improve the security often urge the individuals for alphanumeric combinations, while also being mandated to change passwords on time to time basis. As this process becomes frustrating and complex for the individuals, authenticating individuals at a faster rate and securely keeping in mind the usability aspect is very critical to all industries. The alternative that exits for passwords are one time passcodes, where a five or six digit code is send to the user's device by an SMS and the user use this code along with password to authenticate an action. This process is commonly termed as two screen experience for the user. The issues with this one-time passcode is that if the user changes his mobile number, then he has re-register everything again, the user may be unable to get the SMS because of some network issues, he may not be able to get where the one time passcode on his device is going etc. So there are a lots of usability issues with this approach. Moreover this passcode, even though they are offered for only a short period of time still they are phish-able. Users demand a balance between security and simplicity. This is where the role of biometrics comes into the picture by offering quicker, easier and more robust authentication in a seamless manner. As biometrics is going to be applied for online authentication, amount of biometric data generated by it will be increasing at a very quick pace. To process and analyse such kind of continuous real-time biometric data and outdone it fast enough to get a competitive edge is needed.

One of the greatest challenges of deploying biometric systems has been the cost. A collaboration of various tortuous sensors, costly devices or cameras is needed in order to deploy the biometric technology; this biometric hardware has previously been priced very high. However, with the advancement in computing over a year, such biometric technology has become at stake; indeed, now a days every mobile phone is already equipped with sensors which ease the process of biometric authentication. The mobile phone is today an indispensable companion in both people's private and professional lives. People prefer to use their mobile phone to net banking, pay bills, transfer funds, etc. Thus to use biometric to authenticate a user online, the smartphone applications, will take advantage of the many inbuilt mobile sensors available on mobile devices, open possibility for analyzing and processing new types of generated data, and possess an impact on almost all activities of societal and business life, and include, but are not limited to, mobile marketing, social networks, smart cities, health maintenance, and business processes [3].

Till now, the biometric data are just used for identification and verification of a person. The traditional biometric data processing environments are heavily oriented toward batch operations with extremely high latencies, single-point of failure and were incredibly costly. Furthermore, to analyse this biometric data the traditional approach requires all the biometric

Today 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. But security of critical data over the cloud has become a concern for both cloud service users and providers. Traditional authentication mechanism like password, key generation, encryption mechanism has failed. 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.

In this paper, we are presenting a secure authentication mechanism unlike password or key which can't be hacked easily. Biometrics is an automatic identification of a person by using certain physiological features associated with the person. Biometrics data is unique for every individual. So our project aims at using Biometric data of user for the authentication process.

2. LITERATURE SURVEY

This section of Literature Survey eventually reveals some facts of Biometric Authentication based on the analysis of many authors work as follows:

Chandra ShekharVorugunti [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 next is Verification. In Enrolment process the biometric data is converted into a binary form. The feature extractor then converts the binary string into a set of features. 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. Thus they have provided a service to do heavy weight cryptographic encryption and decryption operation on user's biometric data.

D J Craft [2] reports on fast hardware implementation of lossless data compression algorithms. It proposed Adaptive Lempel-Ziv Algorithm (LZ1 & LZ2). LZ algorithm are symbol based that is they operate one data one character at a time. They achieve compression by locating frequency occurring sequences of such symbol in input data stream. ALDC have two extensions as BLDC & CLDC. BLDC pre-processing works well on only bitmapped image data. CLDC is combination of ALDC & BLDC. The main difference between LZ1 & LZ2 is in the data structure employed & the way reference to sequence are coded.

Cong Li et al. [3] proposed Burrow Wheeler Transformation based DNA sequence data multi-compression using OpenMP & MPI. They proposed data compression (DNA sequence) using fewer bits rather than encoded data to represent information. BWT based DNA compression includes few steps. First DNA sequence data is encoded with 0/1 which has 4 characters. Then BWT transformation is performed over it. Again MTF transformation is performed. Then we compress data with classical algorithm.

Kiran Kumar K et al. [4] 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 minutae and ridges. The method used in this paper has 8 stages. They are gray-level fingerprint image, binarization, thinning, minutae extraction, false minutae, matching scores, ridges extraction, minutae and ridge score fused using strength factor. The block filters preserve the outermost pixels along each ridge.

Jeff Collier [5] proposed a system for developing a software that would address the challenges such as in-memory map/reduce. It also deals with the node that has ability to leave and re-join the cloud by applying compression and image processing algorithms.

Hu Chun et al. [6] have proposed a situation where biometric data is kept encrypted in whole process of transmission and matching. It uses two approaches homomorphic encryption and garbled circuit. It provides highly computing capability. Surender Sharma et al. [7] have introduced health care monitoring system application that provides the patients with necessary healthcare information yet it also gives a chance to threats of intervention that would make the critical data insecure. They have used Body Area wireless sensor network as monitoring component. The cloud based HMA was therefore developed using master slave like pattern, where the master could have generic functions while slave would have functionalities specific to the medical condition. Thus they have utilized biometric encryption for providing protection to the data. Here the user's biometric characteristics work as decryption key here fuzzy extractor scheme has been used to convert the scanned fingerprint data to some random string and an helper string to apply cryptographic techniques. This framework accomplishes both the goals, secure access and data protection.

Krishnaraj Madhavji Sunjiv Soyjaudah [8] discussed about eight points of vulnerabilities that can be hacked. In cloud data is moved dynamically so security is a major concern and there are the problems which arise in the management of biometric data. So a cancellable biometric authentication system is proposed by him. Cancellable Biometric Authentication is a concept in which the original image is first distorted then shared on cloud. This distorted biometric image is used for authentication. This provides security and privacy as the original biometric are never revealed to authentication server. Data Hiding is also done using this technique to overcome the replay attack. This is done by secretly embedding the private information in biometric image.

Dr. Anandhakumar P et al. [9] has addressed the issues that arouse during storing different documents and files and photo contents on Cloud. Huge amount of photos are maintained by cloud providers. Huffman coding cannot achieve high levels of compression also all the binary strings or codes in the encoded data are of different lengths. So it is difficult to decode. The representative signal(RS) based approach is suitable only when images are highly correlated to each other so it fails badly in case of illumination changes. To overcome these drawbacks LZ-77 algorithm is proposed in this paper. Lz-77 replaces the repeatedly occurring data with reference to single copy which is already existing in an uncompressed data stream. It uses length-distance pair to encode the match. As compression is in cloud environment, k-means algorithm is used to transfer up by using Map-Reduce concept. They also proposed an idea for effective compression of photo albums which also reduces the time complexity.

Abdullah A. Albahdal et al.[10] explored the mutual benefits of biometrics technology and cloud computing. Presently cloud providers mainly depend on password authentication to authenticate their clients. However, password based authentication suffers from a lot of problems. The most common criticism of password-based authentication is the lack of authenticity. The major barriers preventing individuals and organizations from taking advantage of the cloud are security and privacy challenges. Cloud storage service model provides clients with a remote storage that comes with many desirable features including on-demand model, scalability, accessibility, and cost reduction. Identity management refers to the administration of users' identities within a system. It includes establishing users' identities, managing users' authentication and authorization, and maintaining users' permissions. The promising features of the cloud are attractive to biometrics systems. These features include the unbounded storage and processing power, elasticity and flexibility, and cost reduction. Biometrics systems can migrate data to storage or processing in the cloud. Biometrics systems rely on computation-intensive processes to perform the different biometric functions such as identification (1:N), verification (1:1), and de-duplication (N:N) process. Biometrics with its strong authentication properties can be leveraged by the cloud to enhance the security of the cloud and to offer new models of service

3. SYSTEM ARCHITECTURE

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 as shown in the Fig. 1

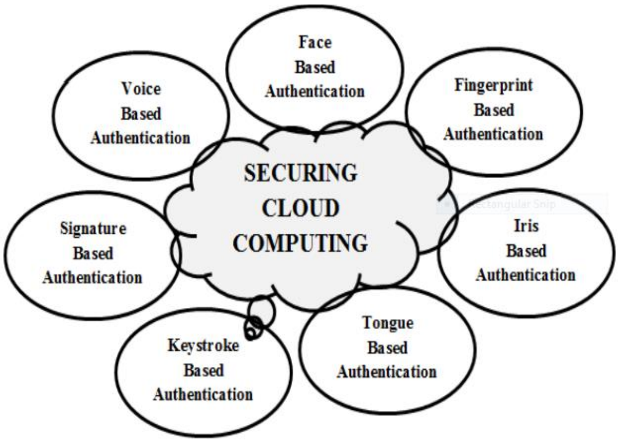
Face Based Authentication
Voice Based Authentication
Fingerprint Based Authentication
SECURING CLOUD COMPUTING
Signature Based Authentication
Iris Based Authentication
Keystroke Based Authentication
Tongue Based Authentication

Figure 1 Biometric Techniques to Secure Cloud Computing

3.1 ENHANCED SECURITY OF CLOUD APPLICATIONS

Cloud based services are usually accessed through a web-based user interface that can either be a web browser or a mobile application. Also, cloud based biometrics is managed by a cloud service provider and is available on demand. The cloud based biometrics includes a server that contains the biometric templates database as well as all the processing data generated during the identification and verification process for cloud users.

Even though biometric traits are unique, problems might arise if unscrupulous individuals gain access to the stored biometric templates database. Biometric authentication takes care of this security threat by utilizing encryption technology. The process of converting the data into a form that cannot be understood by unauthorised individuals is known as encryption whereas converting the data back to its original form so that it can be understood is known as decryption.

The fingerprint images at both the user's end as well as the service provider's end are encrypted for providing better security using an encryption algorithm. Therefore, even if a hacker is able to gain access to a fingerprint image he will not be able to decrypt it to the original image.

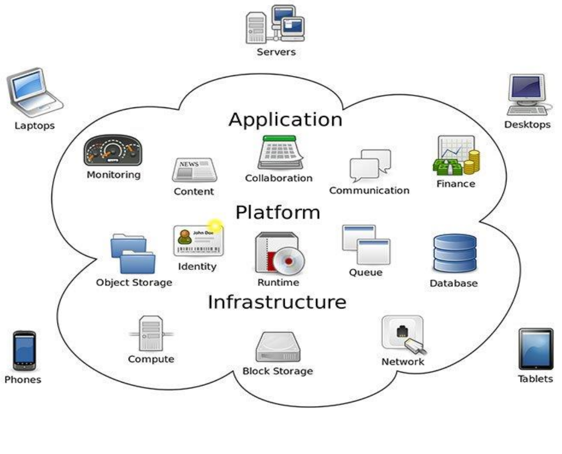

Figure 2 Essential Cloud-based services

A multi finger security model can also be used for increasing cloud services security. In this scheme, the cloud users register with three fingerprint templates of their choice and assign a single digit for each of the three fingers. The fingerprint images, the single digit numbers and the mapping of fingers to numbers are encrypted using an encryption algorithm and stored at the service provider's end. Such a scheme provides a very high level of security as it uses three different inputs from the cloud users and further makes it efficient by applying an encryption algorithm.

3.2 BIOMETRICS

"Biometrics" is a Greek word, based on two words, "bio" meaning life and "metric" meaning to measure. Biometric authentication states the proof of identity of humans by their characteristics or traits. Biometric traits are universally unique. In computer science it is used as a practice of identification. Biometric frameworks permit recognizable proof of people taking into account behavioral or physiological attributes. To accomplish more dependable confirmation or ID we ought to utilize something that truly describes the individual.

Biometric System is a combination of sensors, feature extractor and matching modules which implements biometric recognition algorithms. The sensors scan the biometric trait of the user and produce its digital representation. A quality check is generally performed to ensure that the acquired biometric sample is reliable and can be processed by the subsequent feature extraction and matching modules. The feature extraction module will discard the useless and extraneous data present in the taken sample and extracts useful information called features that can be used for matching.

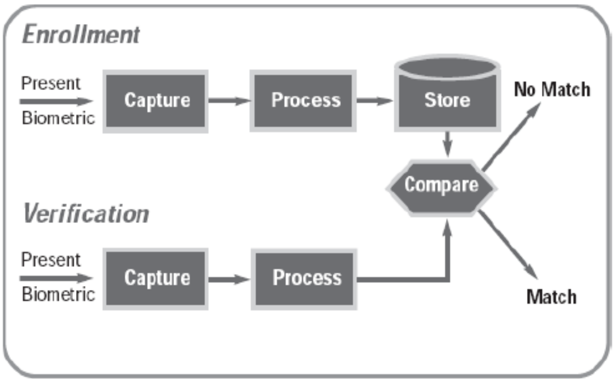

Figure 3 Working of biometric based authentication system.

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. This operation is done in two stages, first is the Enrolment and second is the recognition

In Enrolment stage the biometric information of the person is stored in the database. We are implementing our project to match fingerprint data of user for authentication in cloud. We will store 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. We are using Biometric scanner to extract fingerprint of user. Fingerprint data will be transmitted in the compressed from for security of users Biometric data. There is a matching module to match the fingerprints against the one stored on the database. If the fingerprint matches, it will allow the registered user to login.

3.3 PROPOSED 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.

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.

In general Biometric Authentication scheme consists of two stages:

- Enrolment process.
- 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.

4. CONCLUSIONS

In this paper we discussed cloud computing. It is based on sharing. Cloud service providers provide the services to users on pay only for use strategy. To provide these services efficiently, security is a major concern. To overcome the security issues different types of techniques are used. Biometric techniques are most popular among all the techniques. Biometric authentication techniques use various kinds of sensors. Almost all of the biometric authentication techniques have some drawbacks. So the solution to have a secure channel is to use multi model authentication scheme using more than one biometric technique.

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 "Outsourceable two party privacy preserving biometric authentication," June 4–6, 2014, Kyoto, Japan

[6] The Problem with Passwords: http://thecipherbrief.com/article/problem-passwords, Accessed on 04.02.2016, 7:09 AM.