# A Survey On Biometric Security Technologies From Cloud Computing Perspective

Shivashish Ratnam, Mimzee Gupta, Dr. Ajay S. Singh, Thirunavukkarasu K

**Abstract**: Cloud computing is one of the rising technologies, that takes set of connections users to the next level. Cloud is a technology where resources are paid as per usage rather than owned. One of the major challenges in this technology is Security. Biometric systems provide the answer to ensure that the rendered services are accessed only by a legal user or an authorized user and no one else. Biometric systems recognize users based on behavioral or physiological characteristics. The advantages of such systems over traditional validation methods, such as passwords and IDs, are well known and hence, biometric systems are progressively gaining ground in terms of usage. This paper brings about a new replica of a security system where in users have to offer multiple biometric finger prints during Enrollment for a service. These templates are stored at the cloud provider's section. The users are authenticated based on these finger print designed templates which have to be provided in the order of arbitrary numbers or imaginary numbers that are generated every time continuously. Both finger prints templates and images are present and they provided every time duration are encrypted or modified for enhanced security.

**Keywords:** cloud computing; biometrics; services; technology; Fingerprint; Voice Recognition; Physical biometrics;

## I. INTRODUCTION

Biometric Security is now a days a very familiar and trustworthy security system which has a massive demand today and will not suffer any kind of degression in its want in the upcoming future. The security factor in the biometric security system in highly improvised by concatenating the data with a unique physical quality. The term "biometrics" is infested from the Greek language and is taken up from two special words bio (meaning life) and metric (to examine).Biometrics (a security measure) is the recognition of the humans by the help of their physical traits/behavior. The main purpose of biometrics in Computer science is to serve a method of identification [1]. The system is provided with the biometric identity (like fingerprint or voice sample), which is then real against a stored template. It is an invincible security measure which cannot be defeated by anybody which makes it a significant reason for being given the first preference first while thinking about the security essentials with respect to IT or Cloud Computing. The two different modes in which biometric systems can be used are- Verification by identity: This mode is used when the user is previously enrolled in the system (ID card or login name) In such a case there takes place the comparison between the user's biometric data and the user's data which is already present in the database. Identification (also known as recognition) occurs when the identityof the user is a prior unknown to someone else. In sucha case the user'sbiometric data is compared with all the records available or stored in thedatabase as the details of the user may be present anywhere in the database orthe user may not any info previously stored [2].

.


- *Shivashish Ratnam: Galgotias University, India* shivashishratnam@gmail.com
- *Mimzee Gupta: Galgotias University, India* cutipy.mimzee@gmail.com
- *Dr. Ajay S. Singh: Galgotias University, India* drajay.cse@gmail.com
- *Thirunavukkarasu K: Galgotias University, India* thiruk.me@gmail.com



***Fig. 1.*** *Finger print impression*

## II. AUTHENTICATION PROCESS IN BIOMETRIC SECURITY

### A. Biometrics: An Authentication Tool

Biometrics refers to the identification of an individual identity by making use of the unique physiological uniqueness. The prime motive is to utilize the special unique physical traits of the individual for the identification.Toserve the same purpose of identification of the person various biometric behavior/methods have been developed and are being used for the authentication.Various unique human traits like finger prints, face recognition, tongue impressions and iris are the techniques used for biometric authentication and thus differentiating users from the present working scenarios. Thus a cloud user has to register with these special unique traits (such as iris, finger prints etc.)while Enrollment or using a service. They areusually stored at the cloud service provider's section as templates. Every time when there occurs an entrance, the cloud user is stimulated for the provisioning of his enrolled trait or data which then gets compared with the stored template for authentication. Inspite of the uniqueness of the biometric traits, theproblems arise when someone gains access to the stored templates of the traits.

### B. Working System of Biometric Security

The biometric database of the useris maintained by theauthentication service provider.Cryptographyis used for storing the data in encrypted format on biometrics for securityreasons. Therefore, the user has to be initially enrolled to the biometric system provided by the cloudplatform or service provider and once after the identity registration the biometric authentication details of the person are stored in the source database of cloud. At the time of registration, the authorization details or important detailsentered are also present in encrypted format. Thus firstly the biometric authentication service comes into action instead of the conventional password mechanism whenever a user seeks to use the cloud services. Once authentication is completed, the user is then redirected to the genuine cloud service platform of which he has been provided with the authority.

## III. TYPES OF BIOMETRIC METHODS

In order to safeguardthe data from virus or any other obstacle from entering and expanding, there are some biometric methods which can definitely be adopted as a security measure in cloud computing technologies. Two biometric methods are:

### A. Physical Biometrics

Physiological biometrics is one which is based on size and data extracted from direct measurement of part of the body. The various leadingphysiological biometrics techniques arefingerprint, retina-scan,iris-scan, facial recognition and handgeometry. In Physical Biometrics, the physical impression is used instead of artificial impression for the passwords. The physical impression is quickly scanned and a pathway no matter it gets matched or not.If the impression gets matched,then user advances to the next step for security.

### B. Behavioral Characteristics

Behavioral characteristics are based on how the person reacts to the specific conditions. Behavioral biometrics, in turn, are basedon measurements and data extracted from an action, andin a they measure the characteristics of the human body.Voice recognition, keystroke-scan, and signature-scanare leading and important behavioral biometric technologies present in today's scenario. One ofthe major characteristics of a behavioral biometric isthe inclusion of time as a measure [3]. Only a few out of various biometric methods developed were able to gainapproval.

## IV. PROS AND CONS OF DIFFERENT BIOMETRICS MEASURES

Going hand in hand with its name, Biometrics is a phenomenon which can be trusted most for security purpose. But beside all these myths there are also some merits and demerits of this system.On the basis of authenticity biometrics can be done as following:-

**Fingerprint:-** Fingerprint technology is one such technology which is quite common in today's era and it starts first with the IT industry.Fingerprint starts the concept of biometrics. Today many companies are adopting the biometric security as a finger print scanner for the attendance of their employees. Biometric device keeps the record of the person in terms of their entry and exit in the company.

**Facial Recognition:-** Facial Recognition is a type of unique scan in which the face is to be captured by a device and it scans it as a whole. During the scanning , it draws a grey light on the face and the device completely scans the face. The system thus scans it and puts in beside the screen and as a result , it acts as a gateway of user authentication with password as a facial recognition . Today sometimes airport authorities are using this method when there is a risk of terror . Facial recognition can completely scan the face and something which is inappropriate can be easily taken out .

**Retina Scan:-** Retina scan is based on the blood vessel prototype in the retina of the eye. Retina scan technology is far older than the iris scan technology that also uses a small part of the eye. A retina scan produces at least the same amount of data as that of a fingerprint image. Thus its discrimination rate is sufficient not only for confirmation purpose, but also for detection purpose. In the practical purpose, Retina scan is suitable for applications where the high protection is suitably required and the user's acceptance is generally not a major aspect. Retina scan systems are used in many countries prisons to prove the prisoners when they were about to get released. The check of the eye aliveness is usually not of a significant concern as the method of obtaining the retina blood vessel pattern is rather complicated and requires an operatorto manage.

**Voice Authentication:-** Voice Authentication is a method by which a system can recognize the voice in order to open an encrypted information .Voice recognition is the most successful biometric verification techniques and is used in a wide way. Today Windows are adopting this feature for setting up of locks in a system. Therefore it is almost impossible for any user to break down the password of another user, if he had already adopted this method.[4]

**Facial Scan:-** Facial Scan is one type of scan in which some part of the face is scan in the system. Facial Scan acts as a very powerful and interactive Biometric System . Although it didn't get much popularity as many of them knows about fingerprint scanner rather than anything else. [5]

**Keystroke Dynamics:-** Keystroke dynamics is one such platform which uniquely identify a biometric from its physical structure. Although it can be say that Keystroke Dynamics is much similar as Fingerprint Scanner. The only difference is that in place of fingerscanner it acts as a rhythm track . In keystroke dynamics, the fingers set a pattern and it works accordingly. Therefore keystroke dynamics on the other hand can be called as Pattern lock system which we usually see in Android Mobiles.

## V. PROPOSED SCHEMA IN CLOUD

There are many proposed schema available in the cloud. But we opt for the best. Therefore many features have been adopted which further need to be implemented and as a result it can be assigned in different sections of cloud

computing.The encryption algorithm is applied at three levels.

- Finger print scanner
- Three single digit unique numbers
- Mapping of the number to the other images

The new model can be evaluated at three phases namely

1. Enrollment phase
2. Access phase
3. Matching phase

## VI. CONCLUSION AND FUTURE WORK

Even if the precision of the biometric techniques is not perfect till now, there are many mature biometric systems available now, in order to compete against the previous systems. Proper design and implementation of the biometric system can indeed an increase for overall security, especially the smartcard based solutions seem to be very promising in the near future. There are many numerous conditions that must be taken in account when designing a secure biometric system. First, it is necessary to realize that biometrics are not a secrets. This implies that biometric measurements cannot be used as a capability tokens and it is not secure to generate any cryptographic keys from them. Second, it is necessary to trust the input device and make the communication link protected and stronger. Third, the input device needs to check the liveness of the person being measured at a specific time and the device itself should be confirmed for example by a challenge-response method. In summary, as Biometrics allow for increased security,convenience we can say that fused biometric authentication system can be stated as a novel solution for authenticating users on cloud computing which can be provided as service on cloud and can be worn or swear as a single sign on. Thus this research work gives a detailed view of all the features which is beneficial to the customers and also the further use can leads to expandability of the resources.

## REFERENCES

[1] http://en.wikipedia.org/wiki/Biometrics

[2] http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf.

[3] http://www.indexbiometrics.com/physiological_or_behavioral.htm

[4] http://ntrg.cs.tcd.ie. http://www.sans.org/reading_room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning.

[5] P.Tuylus, E.Verbitskiy, J.Goseling and D.Denteneer, Privacy Protecting Biometric Authentication Systems, An Overview, EUSIPCO 2004: XII European Signal Processing Conference.

[6] Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security – Sowmya, Suryavara, ShuchitaKapoor, ShwetaDhatterwal, RohailaNaaz and Anand Sharma, Modi Institute of Technology and Science, Lakshmangarh, Rajasthan, India- 2011 International Conference on Information and Network Technology IPCSIT vol.4 (2011) IACSIT Press, Singapore.

[7] N.K.Ratha, J.H.Connell and R.Bolle, Enhancing Security and Privacy of Biometric Based Authentication Systems. IBM Systems Journal, 40(3);614-634 2001.

[8] NIST Special Publication 800-145 “The NIST Definition of CloudComputing” Peter Mell Timothy Grance http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[9] http://www.netsecurity.org/secworld.php?id=8922

[10] AnupamTiwari, “CLOUD FORENSICS: CHALLENGES ONLY AHEAD”, Cyber Times International Journal of Technology & Management, Vol. 8 Issue 1, October – March 2015.

[11] Kemal A. Delic, Jeff A. Riley, Enterprise Knowledge Clouds: Next Generation KM Systems?, International Conference on Information, Process, and Knowledge Management, 2009.

[12] "Towards Continuous Cloud Service Assurance for Critical Infrastructure IT". The 2nd International Conference on Future Internet of Things and Cloud (IEEE FiCloud-2014). Retrieved 2014-08-15.

[13] AlbenaAntonova, RoumenNikolov, Conceptual KMS Architecture within Enterprise 2.0 and Cloud Computing, Computing, 2005.

[14] http://ntrg.cs.tcd.ie

[15] Blind Authentication: A secure crypto-Biometric Verification protocol.

[16] http://en.wikipedia.org/wiki/Single_sign-on

[17] NIST Special Publication 800-145 “The NIST Definition Cloud Computing “