Secure Your Cloud Using Part of Yourself: "Biometrics"

[1]Dr. Nikita Yadav, [2]Dr. Garima Yadav
[1]Bhagini Nivedita College, University of Delhi, India
[2]Bharati College, University of Delhi, India

Abstract
Cloud? Yes, cloud is the buzzword in now days. Everyone everywhere is talking about it. Cloud computing has gained popularity very fast because of its incredible advantages some of them involves cost efficient, almost unlimited storage, backup and recovery, automatic software integration, quick deployment, easy access to information and so on. Despite of having all these advantages there is problem or can say challenge in this technology is security. Security you or we can say is the biggest challenge, threat or question to every technology which is faced all over world the world. At present biometric is the answer to this. In this paper we use biometrics to make our cloud secure.

Keywords
Cloud Computing, Biometrics, Security

I. Introduction

The term cloud computing is everywhere .Google drive, Apple iCloud, amazon drive,drop box and etc are common examples of cloud computing which we hear and use in our daily life. Now the question arises what is the cloud? Where is the cloud? Are we in the cloud now? [1]. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive.

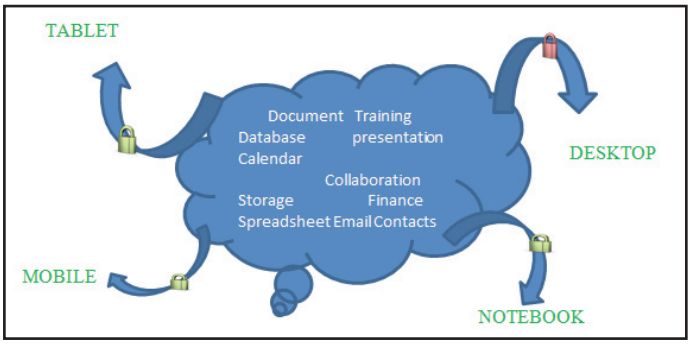

Fig. 1: Cloud Computing

II. How Cloud Works

While working with the cloud one must have the credentials to access your requested services and you will usually receive a monthly invoice for your consumption.The person order services through the Cloud Service Consumer, when he/she log in to a portal (enterprise or public wise). This service has been created by the cloud service provider and can be a simple virtual machine (VM) based on an image, some network components, an application service such as an WebApp environment and a service such as MongoDB. It depends on the provider and type of resources and services.The cloud provider will validate, through the BSS, your request and if the validation is okay (credit card, contract), it will provision the request through the OSS [2]. Fig. 2 represents the simple enrollment process.

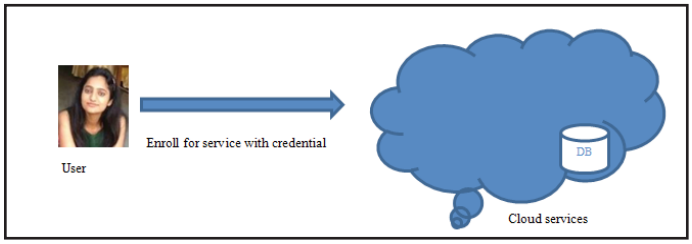

Fig. 2: User Registering With Its Cloud Service Provider

III. Biometrics

Now, at the time when user is enrolling for services came the security.Security?From ancient time to present we have come a long way from "something you know" (e.g., password, Personal identification number- Knowledge based approach), to "something you carry" (e.g., physical key, ID card- token based approach) and to "something you are" (e.g., face, voice)[3]. Suppose if you are using password or any token to prove our authentication thesetwo methods have their disadvantages i.e. your password can be stolen and your token may be lostrespectively. But out of above listed three methods "something you are" is the latest, gaining popularity and used all over the world. Because no can stole from you what you are. This method is known as "Biometrics".

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual. Biometric data could be physical or behavioral body trait of a person.Examples of physical traits include face, fingerprint, iris, palm print, hand geometry and ear shape. Gait, signature and keystroke dynamics are some of the behavioral traits of a person. Biometric traits whether they are physical or behavioral are used because they are unique to the person and can be easily used to differentiate persons from one another. When we use biometric as authenticating tool to enroll in to the cloud service, user register through its biometric traits i.e. hand palm, iris, finger print, face and etc. instead of password or tokens. At the cloud service providers end these traits are stored as templates. Every time person uses its biometric trait to register these trait is compared with the template store at the service providers end, if both get matched then the user is authenticate to use the service otherwise not. Fig3 represents the enrollment process using biometric trait.

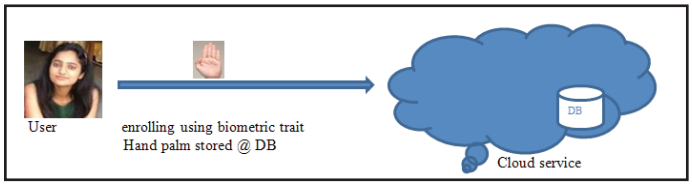

Fig. 3: Enrollment Process Using Biometric Trait

IV. Encryption For More Security

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via theinternet or other computernetworks. During the process of encryption thedigital data or image is converted to another form known as cipher text, which cannot be understood by any other person other than authorized person [4].On other hand decryption

is the process of converting cipher text back to the original form so that it can be understood. The advantage of doing so is that if a hacker gets an access to the image he/she cannot able to decrypt it. Therefore decryption algorithms are very complex. Fig. 4 represents it diagrammatically.

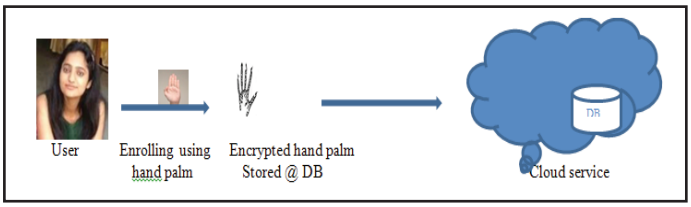

Fig. 4: Biometric Trait Encrypted at User End and Stored at Cloud Service Provider End

This technique, undoubtedly suffers from security weaknesses [5]. Vulnerable storage may lead to an attacker stealing biometric templates and impersonating the legitimate user. The stolen biometric information may compromise other systems [6]. A cloud private matching algorithm is proposed in [7]. Two encrypted images are compared under double encrypted conditions, from the client and from cloud storage.

Instead of having various pitfalls in the above mentioned techniques, there is one more problem which can occur while using cloud computing. It may happen that user may leave the system or portal unlogged and left from there. At this point an unauthenticated person can use the service or may miss use them. To overcome this problem we can use soft biometric traits with hard biometric traits.

V. Soft Biometric Traits for Continous Authentication

Soft biometric traits are defined as "those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals" [8]. These traits include gender, ethnicity, and color of eye/skin/hair, height, weight, and SMT (scars, marks, and tattoos). While soft biometric traits do not have sufficient discriminatory information to fully authenticate the user, it has been shown that they can improve system login security when combined with hard biometric traits (e.g., fingerprint, face, iris, palm vein, etc.) [9-10].

In order to use soft biometric trait to check continuous authentication of the person the cloud service provider can ask for soft biometric trait certainly at any point, if the soft biometric trait is unavailable then asked for re-login.To make this work when user enroll using its hard biometric traits at the same time the soft biometric traits of the person are also get stored. At any certain point cloud service provider can check authentication of person by checking its soft biometric trait(e.g.: color of clothes, skin color, hair color, hair style and etc.).While using soft biometric traits to check continuous authentication cloud service provider system should be robust with respect to user's posture in front of the workstation and it also has the capability for enrollment template update and re-login authentication [11]. There should be one or more camera at users end and these were stored at cloud service provider database.

VI. Conclusion

We have tried to use hard and soft biometric traits to increase the security level of cloud computing and also tried to check whether an authenticated person is using the service of cloud service provider all the time. Use of both hard and soft biometric trait promises high security.

Refrences

[1] [Online] Available: http://in.pcmag.com/networking-communications-software/38970/feature/what-is- cloud-computing
[2] [Online] Available: http://www.thoughtsoncloud.com/2014/02/how-does-cloud-computing-work/
[3] IBM Corporation,"The Consideration of Data Security in a Computer Environment", Technical Report G520-2169, IBM, White Plains, USA, 1970
[4] [Online] Available: http://searchsecurity.techtarget.com/definition/encryption
[5] P.Tuylus, E.Verbitskiy, J.Goseling, D.Denteneer,"Privacy Protecting Biometric Authentication Systems: An Overview", EUSIPCO 2004: XII European Signal Processing Conference
[6] David Gonzalez Martnez, Francisco Javier Gonzalez Castano, Telematics Engineering Department, University of Vigo, Spain.-Secure Crypto-Biometric System for Cloud Computing
[7] Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security – Sowmya, Suryavara, Shuchita Kapoor, Shweta Dhatterwal, 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.
[8] A. K. Jain, S. C. Dass, K. Nandakumar,"Can soft biometric traits assist user recognition?," Proc. SPIE, Vol. 5404, pp. 561–572, 2004.
[9] A. Altinok, M. Turk,"Temporal integration for continuous multimodal biometrics", In Proc. Workshop on Multimodal User Authentication, 2003, pp. 131–137.
[10] T. Sim, S. Zhang, R. Janakiraman, S. Kumar,"Continuous verifi- cation using multimodal biometrics," IEEE Trans. Pattern Anal. Mach. Intell., Vol. 29, No. 4, pp. 687–700, Apr. 2007.
[11] [Online] Available: http://www.cse.msu.edu/biometrics/Publications/SoftBiometrics/NiinumaParkJain_SoftBiometricTraitsContinuousUserAuthentication_TIFS10.pdf

Dr. Garima Yadav received my B.Sc. degree in physics from Shivaji College, University of Delhi, India, in 2007, the Master's degree in Computer's (M.C.A.) from Maharishi Dayanand University, Rohtak, India and the Ph.D. degree in Biometrics in 2014. I am teaching as Assistant professor in Bharati College (University of Delhi) since 2014. My research interests include Biometrics and Cloud Computing.

Dr. Nikita Yadav received her B.Sc. degree in Computer Science from Bhaskar Acharya College of Applied Science, University of Delhi, India, in 2008, the Master's degree in Computer's (M.C.A.) from Maharishi Dayanand University, Rohtak, India and the Ph.D. degree in Cloud Computing in 2014. Now, teaching as Assistant professor in Bhagni Nivedita College (University of Delhi) since 2011. Her research interests include Cloud Computing and E-Governance.