Journal of Biometrics & Biostatistics
ISSN: 2155-6180

Naveed and Batool, J Biom Biostat 2015, 6:5
DOI: 10.4172/2155-6180.1000258

Perspective Open Access

Biometric Authentication in Cloud Computing

Ghazal Naveed* and Rakhshanda Batool

Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan

Abstract

Information and telecommunication technology (ICT) has penetrated deep into the human lives and is affecting human life style in different aspects. The rapid growth in ICT has embarked improvement in computing devices and computing techniques. Currently cloud computing is one of the most hyped innovation. It has several positive impacts like reduce cost, increase throughput, ease of use but it also have certain security issues that must be dealt with carefully. There are several techniques that can be used to overcome this major problem. In this paper will analyses biometric authentication in cloud computing, its various techniques and how they are helpful in reducing the security threats. It provides a comprehensive and structured overview of biometric authentication for enhancing cloud security.

Keywords: Cloud computing, Security; Data access; Authorized user; Biometric authentication; Cloud Service Provider (CSP)

Introduction

For the ease of users, concept of cloud computing took popularity in 1990's though its concepts lasts back to 1960s [1]. Cloud Computing refers to provision of scalable and IT related services to the users through internet. It is a technique of computing in which dynamically scalable and IT related resources are provided as a service through Internet. This model permits general, supportive, on-interest system right to use to a common group of configurable figuring assets. These resources are rapidly allocated and unconfined with a minor organization's effort [2]. Resources may include systems, servers, application programs or any kind of administrative programs.

It provides 3 different kinds of service models:

1. Software as a service has the ability to provide user any software running on a cloud substructure.

2. Platform can also be provided as a service. In this any kind of platform (i.e. tools, library, services).

is provided as a service of which user has no control but he/she can use it.

3. Infrastructure as a service facilitates the user by providing computing resources where user can run the software without having control on underlying infrastructure but has control over the operating system being used [1].

Four deployment models are used in cloud computing:

1. Public Cloud model facilitates general public and is owned by a specific organization.

2. Community cloud is shared by several users.

3. Private cloud facilitates a private organization.

4. Hybrid cloud structure consists of two or more than two cloud models [2].

Services of cloud computing are being provided by dierent companies known as Cloud Service Providers (CSPs). CSPs provide the services to users on pay only for use strategy [3]. Cloud Computing faces various types of security concerns that include virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication and password [4]. Cloud computing platform has not provided appropriate physical protection procedures, and all protection mechanisms depend extraordinarily on the mechanism of au-thenticating the user. User authentication calls for an extremely assured security.

To solve security issues in cloud computing different techniques are being used. One of the authentica-tion mechanisms is password authentication. Most clients pick something easy to memorize, for example, telephone number, most precious pleasures and name as their passwords. These things are effortlessly to retain. Thus, adversary can assemble a chart of noteworthy disputes to transgress framework. This process is known as dictionary attack. Another technique is smart card based authentication. It is a two factor authentication. In the first influence, clients' examination accreditations are secured in the smart card and in second influence the card is being safeguarded by using a password. The two components needn't bother with the server to store a secret key record. The drawback of this technique is that it is not a basic gadget, and the card reader considers an additional cost. It additionally requires extra mid-dleware application to acquire a match between smart card and correspondence models. Most important of these techniques is biometric authentication. It is a form of authentication in which physiological traits of human beings are used to identify or verify the authenticated user [5] (Figure 1).

Biometrics is a Greek word, based on two words, bio meaning life and metric meaning to measure. Biometrics also known as biometric authentication states the proof of identity of humans by their char-acteristics or traits. 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 ac-complish more dependable confirmation or ID we ought to utilize something that truly describes the individual.

Biometric techniques are largely centred on face, fingerprint

***Corresponding author:** Ghazal Naveed, Assistant Professor, Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan, Tel: +92-51-8354444; E-mail: ghazzalnaveed@gmail.com

Received September 14, 2015; **Accepted** September 21, 2015; **Published** October 05, 2015

Citation: Naveed G, Batool R (2015) Biometric Authentication in Cloud Computing. J Biom Biostat 6: 258. doi:10.4172/2155-6180.1000258

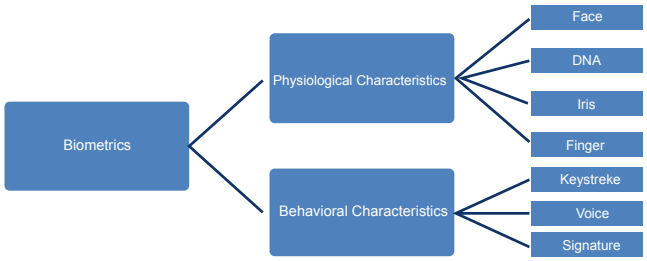

Figure 1: Physiological and behavioral biometric Traits [4].

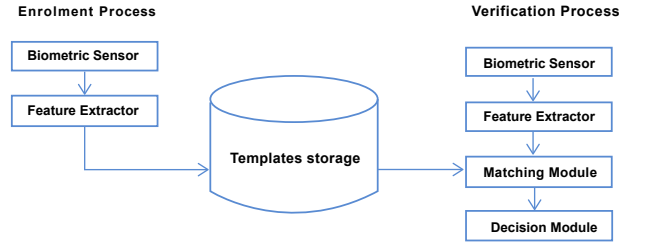

Figure 2: Biometric Authentication Mechanism [7].

and iris detection, verification and identifi-cation systems. Normally detection is the first step in vision procedures. In detection process, system only checks whether face, iris, fingerprint exists for reading procedure and do not match with the ex- isting data. After registration when the user wants to use the service of cloud, detection is followed by the verification process. During this process data detected by the system is matched with the already existing data of the individuals. If any match occurs then user is authorized to use the service otherwise an error message is sent to the user. Biometrics deal with programmed approaches including character check or distinguishing proof on the standard of quantifiable physiological or behavioral qualities, for example, a finger impression or a voice test [6]. In this paper biometric authentication will be discussed in detail (Figure 2).

Related Work

In this survey paper we will analyse dierent kinds of biometric authentication schemes that are being used by various CSPS, their working and also examine the most authenticated technique.

Finger Prints Recognition

Fingerprint refers to an arrangement of elevations and valleys on the exteriors of the finger whose formation is firm. Fingerprint patterns of twins are different from each other [7]. Arrangement of the rims and structures do not change during the course of the lifespan of the human beings unless there is any noteworthy injury that crafts an everlasting scratch [8]. Fingerprint recognition refers to the mech- anized process of ascertaining the uniqueness of a single centred on the evaluation of two impressions. Fingerprint recognition is very famous because it is easy to use, an old method and is highly acceptable in the whole world. It is referred to the computerized way to validate a match between two human fingerprints [9]. The aridity, wetness of fingers and dirty fingers can disturb the scheme and result in inaccuracy.

Fingerprint sensors are used in this technique. They provide a scanned image of the finger. A unique password is created on the basis of fingerprint. Image and password both are stored in the database of the CSP. After registration when the user wants to use the service again, his/her fingerprint is sensed by the sensor and is sent to CSP where matching process is done with the already stored image. If the password of the read finger is valid only then the user can be allowed to use the desired service [10,11].

Facial Recognition

Face is being used as a biometric recognition as traits of face differ from person to person. This is a discrete and is suitable for furtive recognition applications. In face recognition technique features of the face are extracted. Sometimes 2-dimensional image of the face is taken and then stored in the database. In verification procedure 2-dimensional facial features being extracted are matched by the already stored template by using a match engine.

It is preferred that this mechanism should be automatic. The system automatically detects the face, takes its image, and after extracting the features saves it in the data base [8]. It is a cheap technology and gives a quick identification response [12]. It encounters a major problem that as face is referred as a social organ, its expressions are being changed [4].

Iris Recognition

Iris is a circular part surrounding the pupil inside the human eye. It consists of different complex arrangements and is green, blue, black or grey in color. Iris recognition is a technique used to recognize individuals based on unique arrangements in iris. Patterns present in iris are recognizable and are unique to every human. It is used an important biometric recognition technique [4].

In this mechanism identification and verification processes are carried out. In identification process im- age of eye is taken using a digital camera of high resolution. Image can be processed by using infrared or visible waves. It is stored in database of the CSP. In verification process special program is used by the computer to check whether the image taken match with the already stored image of the iris or not. Computer program used for matching purpose is called a matching engine. It has a high computational power and can process millions of images for matching per second.

Accuracy of iris recognition is more as compared to finger print recognition but less precise than retina recognition. It is less insensitive as compared to the retina recognition as iris is easily visible from a distance of a few meters. Twins also possess different iris structures. This technique provides a secondary verification. In this verification iris is subjected to light medium as reactions of the iris changes in light and these responses are also different [13].

Conclusion

For getting accurate results iris should not be far than a few meters from the camera and it must be ensured that the iris must be stationary. Different procedures are used to ensure that the image is real instead

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability
Face	H	L	M	H
Facial Thermogram	H	H	L	H
Finger print	M	H	H	M
Iris	H	H	H	M
Retina	H	H	M	L
Voice	M	L	L	M

Table 1: Comparison of Different Biometric Techniques.

Method	Function mechanism	Advantages	Disadvantages
Finger print	Difference between human finger prints	Very low error rate, being used for over 10 years	Dirty or damaged fingers can affect accuracy
Iris	Using laser or infrared beam	Very reliable with low error rate	Members phobia to expose eyes to light
Facial	Using face expressions and physical measures	Simply accepted by users	Not much accurate due to changing facial expressions
Retina	Imaging of retina	Very reliable with low error rate	Members phobia to expose eyes to light

Table 2: Comparison of various Biometric methods used in cloud computing.

of a photograph. The image can be vague if contact lens is being used. Ensure that reflections should not be produced by the light source. If it happens image can be unclear. Certain sorts of contact lenses and glasses can darken the iris design [14]. The comparison of various biometric techniques used in cloud computing has been shown in Tables 1 and 2 [15].

References

1. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Futur Gener Comput Syst 28: 583-592.
2. Peter M, Timothy G (2011) The NIST Definition of Cloud Computing. NIST Special Publication, USA.
3. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Futur Gener Comput Syst 25: 599-616.
4. Deka GC (2014) Handbook of Research on Securing Cloud-Based Databases with Biometric. National Institute of Technology Rourkela, India.
5. Yassin A, Jin H, Ibrahim A, Qiang W, Zou D. Efficient password-based two factors authentication in cloud computing. Int J Secur its Appl 6.
6. Li H (2012) Advanced topics in Biometrics. Institute for Infocomm Research, Singapore.
7. Wong KS, Kim MH (2012) Towards Biometric-Based Authentication for Cloud Computing. In 2nd International Conference on Cloud Computing and Services Science.
8. Vallabhu H, Satyanarayana R (2012) Biometric Authentication as a Service on Cloud: Novel Solution. Int J Soft Comput Eng 2: 163-165.
9. Edward Guillen MM, Alfonso L (2012) Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network. Proc World Congr Eng Comput Sci 2.
10. Al-hamami H, Al-juneidi JY (2015) Secure Mobile Cloud Computing Based-On Fingerprint. International Journal of Networks and Applications 5: 41-53.
11. Lakhmi CJ, Halici U, Hayashi I, Lee SB, Tsutsui S (1999) Intelligent Biometric Techniques in Fingerprint and Face Recognition. CRC Press.
12. Pawle A, Pawar AP (2013) Face Recognition System (FRS) on Cloud Computing for User Authentication. IJSCE 3: 189- 192.
13. Kresimir MG, Delac I (2004) A Survey of Biometric Recognition Methods, Proc. of the 46th International. Symposium Electronics in Marine. ELMAR-2004, Zadar, Croatia.
14. Teo V (2011) Mobile Cloud Computing for Data-Intensive Applications.
15. Banirostam H, Shamsinezhad E, Banirostam T (2013) Functional Control of Users by Biometric Behavior Features in Cloud Computing. 4th Int Conf Intell Syst Model Simul USA.