Biometric Authentication in Cloud Computing

Rakhshanda Batool
COMSATS Institute of Information Technology
44000, Park Road
Islamabad, Pakistan

Ghazal Naveed
COMSATS Institute of Information Technology
44000, Park Road
Islamabad, Pakistan

Abdulhaq Khan
COMSATS Institute of Information Technology
44000, Park Road
Islamabad, Pakistan

ABSTRACT
In 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 reduced cost, increased throughput, ease of use but it also had 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 we will analyse biometric authentication in cloud computing, it's 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
Keywords Cloud computing, Security, Data access, Authorized user, Biometric authentication, Cloud Service Provider (CSP)

1. INTRODUCTION
Concept of cloud computing took popularity in 1990's though its concepts lasts back to 1960's[1]. Cloud Computing refers to provision of scalable and IT related services to the users through Internet. Itis a technique of computing in which dynamically scalable and IT related resources are provided as a service through Internet. This model permits general, supportive and easy to use system. The resources in cloud computing are rapidly allocated and are unconfined with a minor organization's effort[2]. Resources may include systems, servers, application programs or any kind of administrative programs.

1.1 Service Models of Cloud Computing
It provides 3 different kinds of service models.

1.1.1 Software as a Service (SaaS)
It has the ability to provide user any software running on a cloud substructure. Software is deployed over the internet. In this model customers licenses the applications and the cloud service providers provide the required facility to the end users when they require[3]. Examples may include web browsers and google docs[4].

1.1.2 Platform as a Service (PaaS)
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[5]. User can easily generate applications by using PaaS provided by CSP[6]. Mostly virtual machines are used in this case. Most preferably various kinds of tools and applications are deployed to facilitate the users [4].

1.1.3 Infrastructure as a Service (IaaS)
Infrastructure 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]. IaaS may include IT resources such as severs, networking and storage. Users get access to the infrastructure with the help of virtual machines. It provides an elastic architecture which offers high rate of availability[7].

Four deployment models are used in cloud computing.

- Public Cloud model facilitates general public and is owned by a specific organization.
- Community cloud is shared by several users.
- Private cloud facilitates a private organization. They can be secured privately[8].
- Hybrid cloud structure consists of two or more than two cloud models[2].

Services of cloud computing are being provided by different companies known as Cloud Service Providers (CSPs). CSPs provide the services to users on pay only for use strategy.[5]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 [9].Cloud computing platform has not provided appropriate physical protection procedures, and all protection mechanisms depend extraordinarily on the mechanism of authenticating the user. User authentication calls for an extremely assured security.

Security issues may include following issues[6][1].

- Data mobility
- Availability of data
- Backup of data
- Access of data
- Multi-tenancy
- Lack of standardization
- Control over life cycle of data

To solve security issues in cloud computing different techniques are being used. One of the authentication mechanisms is password authentication. Most clients pick something easy to memorize, for example, telephone numbers, good memories, and names as their passwords. These passwords are very easy to remember. Thus, adversary can easily assemble a chart of important names or numbers to intervene the security. This process is known as dictionary attack. Another technique is smart card based authentication.

It is a two factor authentication. In the first factor, clients' accreditations are secured in the smart card after examining them and in second factor the card is being safeguarded by using a password. The two components don't need to cause any problem 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 middleware application to acquire a match between smart card and correspondence models. Another most important technique is biometric authentication technique. It is a form of authentication in which physiological traits of human beings are used to identify or verify the authenticated user [10]. Figure 1 depicts the physiological and behavioral biometric traits of human beings[9].

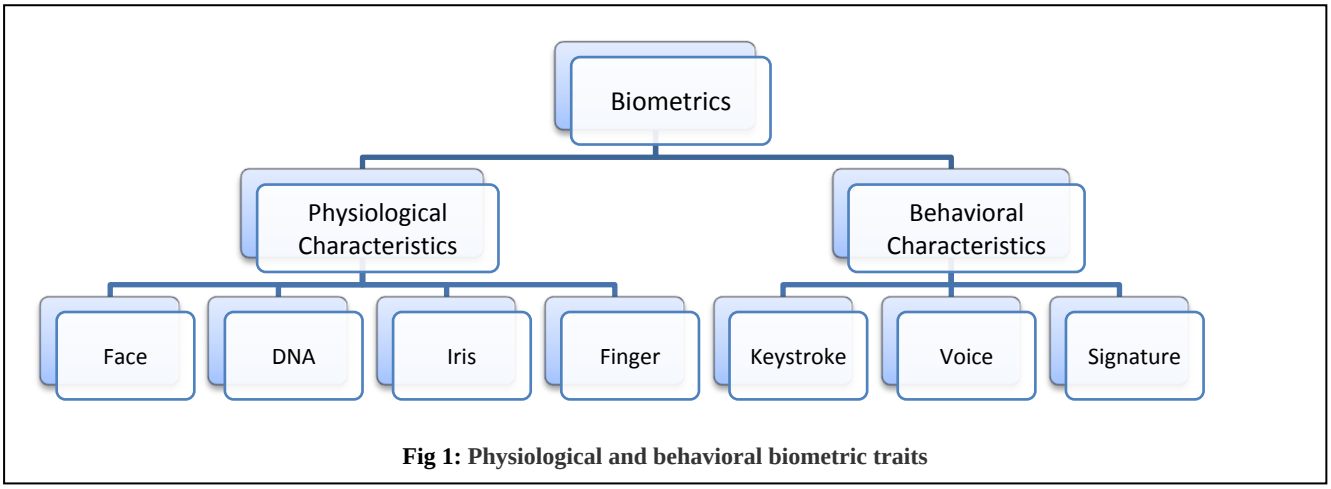

Fig 1: Physiological and behavioral biometric traits

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 techniques are largely centred on face, fingerprint and iris detection, verification and identification 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 existing 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[11]. A Biometric system consists of four steps including sensor module, feature extraction, matching module and decision module[12].Figure II shows the enrolment and verification process for biometric authentication in detail[7].

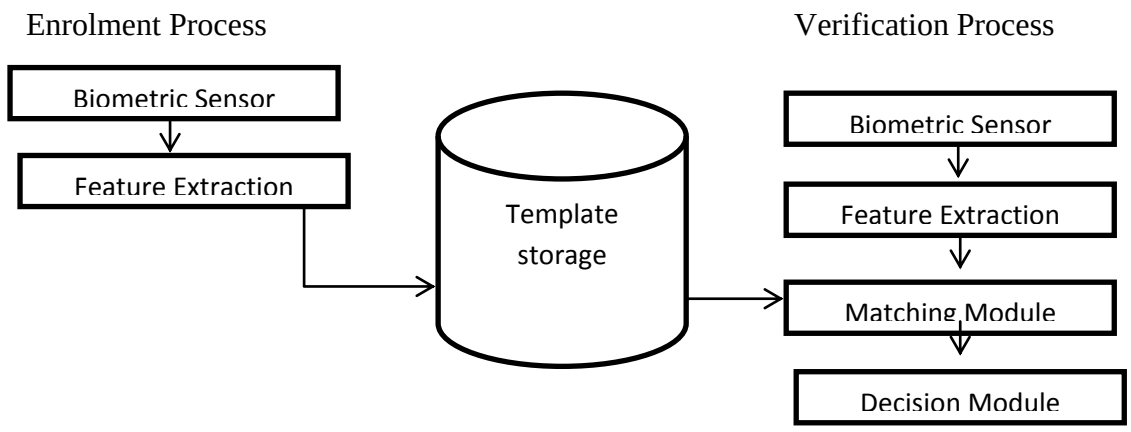

Fig. 2. Biometric Authentication Mechanism

3. RELATED WORK

In this survey paper we will analyze different kinds of biometric authentication schemes that are being used by various CSPS, their working in detail.

3.1 Finger prints Recognition

Fingerprint refers to an arrangement of raises and vales on the exteriors of the finger whose formation is stable[14]. Fingerprint patterns of twins are different from each other[9]. Arrangement of the rims and structures do not change during the course of the lifespan of the human being sunless there is any noteworthy injury that crafts an everlasting scratch[15]. Fingerprint recognition refers to the mechanized process of determining the uniqueness of a human being on the evaluation of two impressions. Fingerprint recognition is a well-known technique 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.[16] The dryness/wetness of fingers and dirty fingers can disturb the scheme and result in inaccuracy[17].

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[8][14].

3.2 Facial Recognition

Face is being used as a biometric recognition as traits of face differ from person to person. This is a distinct feature of users and is suitable for secret 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. Complexion of the user is also quantized[18].

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 [15]. It is a cheap technology and gives a quick identification response[19]. It encounters a major problem that face is referred as a social organ so its expressions are being changed from time to time [9].

3.3 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 as an important biometric recognition technique [9]. It is highly reliable in secured areas.

In this mechanism identification and verification processes are carried out. In identification process image 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].

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 of a photograph. The image can be imprecise 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 [21].

Table I shows a summary of biometric techniques used in cloud computing [20]. The comparison of various biometric techniques on the basis of their characteristics has been shown in table II[22].

Table 1: Details of different biometric techniques

Method	Function mechanism	Advantages	Disadvantages
Finger print	Difference between human fingerprints	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 on basis of different characteristics

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability
Face	H	L	M	H
Fingerprint	M	H	H	M
Iris	H	H	H	M
Retina	H	H	M	L

4. CONCLUSION

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.

5. REFERENCES

[1] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.

[2] P. Mell and T. Grance, "Final Version of NIST Cloud Computing Definition Published."

[3] A. Prasanth, M. Bajpei, V. Shrivastava, and R. G. Mishra, "Cloud Computing : A Survey of Associated Services Cloud Computing : A Survey of Associated Services," vol. 13, pp. 1–15.

[4] A. Shakeabubakor, "Cloud Computing Services and Applications to Improve Productivity of University Researchers," Int. J. Inf. Electron. Eng., vol. 5, no. 2, pp. 153–157, 2015.

[5] R. Buyya, R. Buyya, C. S. Yeo, C. S. Yeo, S. Venugopal, S. Venugopal, J. Broberg, J. Broberg, I. Brandic, and I. Brandic, "Cloud computing and emerging IT

[6] platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Futur. Gener. Comput. Syst.*, vol. 25, no. 6, p. 17, Jun. 2009.

[7] J. Kataria, "International Journal of Advanced Research in Computer Science and Software Engineering Exploring cloud computing and identification of its security issues," vol. 3, no. 5, pp. 1116–1119, 2013.

[8] N. Serrano, G. Gallardo, and J. Hernantes, "Infrastructure as a Service and Cloud Technologies," 2015.

[9] A. H. Al-hamami and J. Y. Al-juneidi, "Secure Mobile Cloud Computing Based-On Fingerprint," vol. 5, no. 2, pp. 23–27, 2015.

[10] G. C. Deka, *Handbook of Research on Securing Cloud-Based Databases with Biometric*.

[11] A. a. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Efficient password-based two factors authentication in cloud computing," Int. J. Secur. its Appl., vol. 6, no. 2, pp. 143–148, 2012.

[12] K.-A. T. Haizhou Li, Advanced topics in Biometrics. 2012.

[13] S. D. Deshpande, "Advances in Computational Research *Review Paper On Introduction Of Various Biometric Areas*," vol. 7, no. 1, p. 9085, 2015.

[14] K.-S. W. and M.-H. Kim, "TOWARDS BIOMETRIC-BASED AUTHENTICATION FOR CLOUD COMPUTING," in *2nd International Conference on Cloud Computing and Services Science*, p. pages 501–510.

[15] *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. CRC Press, 1999.

[16] H. Vallabhu and R. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," *Int. J. Soft Comput. Eng.*, vol. 2, no. 4, pp. 163–165, 2012.

[17] K. M. and M. M. Edward Guillen, Lina Alfonso, "Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network," *Proc. World Congr. Eng. Comput. Sci.*, 2012.

[18] "Secure Mobile Cloud Computing Based-On Fingerprint." [Online]. Available: http://v1.wcsit.org/media/pub/2015/vol.5.no.2/Secure Mobile Cloud Computing Based-On Fingerprint.pdf. [Accessed: 24-May-2015].

[19] M. G. Kim, H. M. Moon, Y. Chung, and S. B. Pan, "A survey and proposed framework on the soft biometrics technique for human identification in intelligent video surveillance system," *J. Biomed. Biotechnol.*, vol. 2012, 2012.

[20] A. A. Pawle and V. P. Pawar, "Face Recognition System (FRS) on Cloud Computing for User Authentication," no. 4, pp. 189–192, 2013.

[21] M. G. Kresimir Delac I, "A SURVEY OF BIOMETRIC RECOGNITION METHODS," *46th Int. SyrnPoSium Electron. Mar.*, 2004.

[22] V. Teo, "Mobile Cloud Computing for Data-Intensive Applications," *Cscmuedu*, pp. 1–9, 2011.

[23] E. S. Hamid Banirostam, "Functional Control of Users by Biometric Behavior Features in Cloud Computing," *4th Int. Conf. Intell. Syst. Model. Simul.*, 2013.