Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

A Study of Different Biometric Authentication Techniques in Cloud Computing

Akshay A. Pawle
Computer Science Dept, COCSIT,
Latur, Maharashtra, India

Vrushsen P. Pawar
Joint Director, WALMI,
Aurangabad, Maharashtra, India

***Abstract* — Cloud computing is a new technology, which is rising rapidly in the market. In cloud computing many computers and servers are connected and are accessed via internet. Using cloud computing we access data, files, resources, application software, operating systems, databases, web servers etc. from anywhere at any time via internet. Cloud computing gets more work done in less time, with less people and with shared hardware and software. So, it gives great throughput with reduce cost. As cloud computing is based on sharing, it is necessary to allow only authorized users in cloud. In short, security is major concern in cloud computing. For authentication different traditional and biometrics techniques are used. Traditional techniques like password, OTP are easily attackable. So, researchers move to biometric techniques. Biometric techniques are more secure as it depends upon physiological and behavioral characteristics of user. This paper is a brief overview of different biometric authentication techniques used in cloud computing with their proposed methods and advantages.**

Keywords* — *Authentication, Cloud, Biometrics, Security, Identification, Verification

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The architecture of cloud computing is dependent on three core concepts namely, service models (SaaS, PaaS and IaaS), deployment models (public, private, community and hybrid) and several essential characteristics.

Biometric Security is now days a very familiar and trustworthy security system which has a massive demand today and will not suffer any kind of digression in its want in the upcoming future [2].

II. CLOUD COMPUTING

Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era [3]. The term cloud refers to a network or internet. In other words, we can say that the cloud is something, which is present at remote location. Cloud computing is also called as "the cloud". Collection of computers and servers which are globally accessible through internet is called, "Cloud Computing". Cloud computing is the delivery of on-demand computing resources–everything from applications to data centers – over the internet on a pay for use basis. The architecture of cloud as shown in fig. 1,

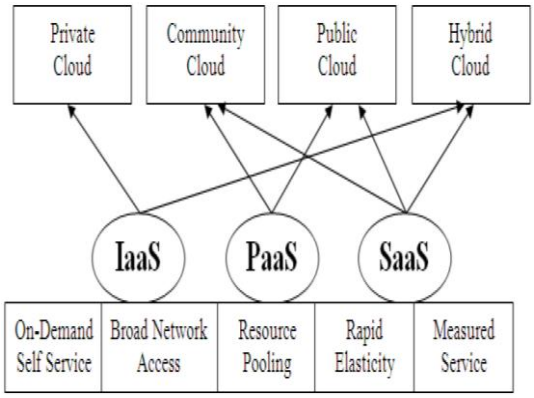

Fig. 1 – Cloud Architecture

A. *Service Models*

SaaS, PaaS and IaaS are the basic service models of cloud computing,

- SaaS – Software-as-a-Service (SaaS) is a way of providing software through the Internet.
- PaaS – Platform-as-a-Service (PaaS) provides a platform in which to develop software applications.
- IaaS – Main objective of any company is to reduce time and money. Infrastructure-as-a-Service (IaaS) model is used to fulfill these primary objectives.

B. *Deployment Models*

The cloud computing is based on several service models. These Deployment model define the type of access to the cloud. These deployment models are Public, Private, Community and Hybrid.

- Public – This type of cloud model is available for all users.
- Private – This type of cloud model is available only for private company users.
- Community – This type of cloud model is shared by several companies and supports to a specific group.
- Hybrid – This type of cloud model is a combination of two or more clouds.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

C. *Essential Characteristics*

The essential characteristics of the cloud computing model were defined by the National Institute of Standards and technology (NIST): On-demand self-service, Broad network access, Rapid elasticity, Measured service, Resource pooling.

D. *Merits of Cloud Computing*

There are several merits of cloud computing, some of them are listed below:

- Up to date Software – With SaaS, the new versions of the software needed to run the business are made available to all customers as soon as they're released.
- Flexibility – Cloud-based services are useful for businesses with growing or fluctuating demands.
- Cost Effective – There is no need to purchase equipment and other utilities to operate business.
- 24/7 Availability – If internet connection is available then user can access cloud services at any time.
- Mobility – Users can access any cloud services from any location of the world.
- Environment friendly – Because of fewer data centers worldwide remain so less impact on the environment.

E. *Challenges in Cloud Computing*

The Cloud Security Alliance (CSA) has put together a list of most severe threats to cloud computing in 2016 [4] as shown in fig. 2,

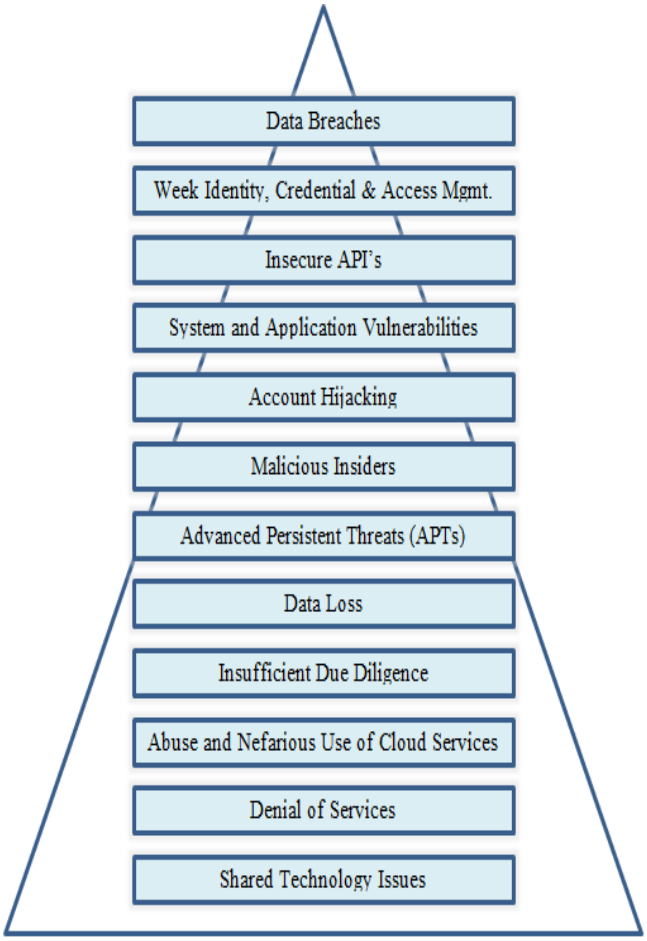

Fig. 2 – Top Cloud Computing Threats in 2016

III. BIOMETRICS

The term biometrics is derived from the Greek words bio meaning "life" and metrics meaning "to measure" [5]. Main role of biometrics is authentication and provide access only to authorized user. Biometric is the measurement and statistical analysis of people's physical and behavioral characteristics.

- Physiological characteristics: It is the structural information of the human body such as face, fingerprints, Iris, hand or DNA.
- Behavioral characteristics: It is the uniquely identifying and measurable patterns in human activities such as keystroke, voice or signature.

Identification system and Verification (authentication) system are two categories of biometric system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

A. *Classification of Biometric Techniques*

Depending upon characteristics of biometric, classification of different biometric techniques as shown in fig. 3,

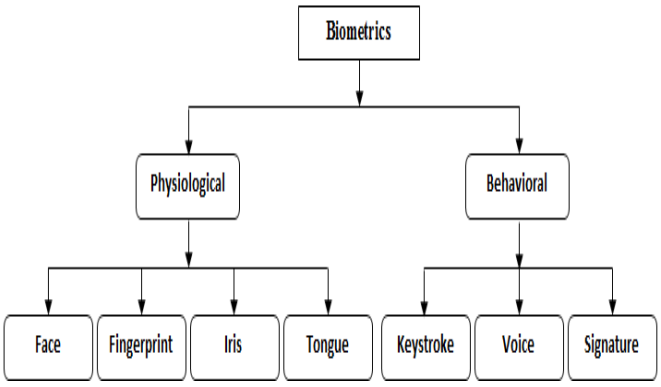

Fig. 3 – Classification of Biometric Techniques

B. *Basic Structure of Biometric System*

Basic structure of biometric system as shown in fig. 4,

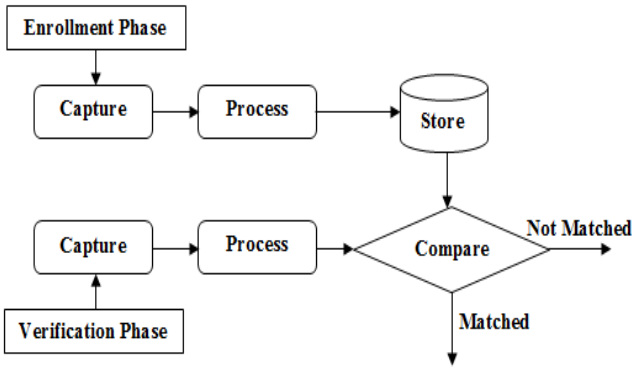

Fig. 4 – Basic Structure of Biometric System

Any biometric system mainly consists of two phases namely, enrollment and verification.

- Enrollment Phase – It consist of three stages i.e. capture, process and store. In capture stage, biometric sample is captured by using camera or scanner. In processing stage, extract different features from capture biometric sample by using different algorithms. In store stage, extracted features from biometric sample are stored on storage medium for further recognition or comparison purpose.
- Verification phase – It also consist of three stages i.e. capture, process and compare. This phase mainly used for matching extracted features of captured biometric sample with stored features. If matched then verification is successful otherwise access is not allowed.

Table I shows comparative study of different biometric techniques based on different parameters:

Table I. Comparative analysis of biometric techniques

Parameters	Biometric Techniques	Face	Fingerprint	Iris	Tongue	Keystroke	Voice	Signature
Accuracy		Medium Low	High	High	High	Low	Medium	Low
Cost		Medium	Medium	High	High	Low	Medium	Medium
Device		Camera	Scanner	Camera	Camera	Keyboard	Microphone	Optic Pen, Touch Panel
Interference		Facial Expression, Glasses	Injury, Dirtiness, Roughness	Glasses	Fungous Infection	Tiredness, Mood	Noise, Cold	Changeable or Easy Signature
Reliability		High	High	Very High	High	Low	High	High
Acceptance		High	Medium	Medium Low	Medium	Low	High	High
Stability		Medium	High	High	High	Medium Low	Medium Low	Medium Low
Identification and Authentication		Both	Both	Both	Both	Authentication	Authentication	Both

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

IV. BIOMETRICS IN CLOUD COMPUTING

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 fig. 5,

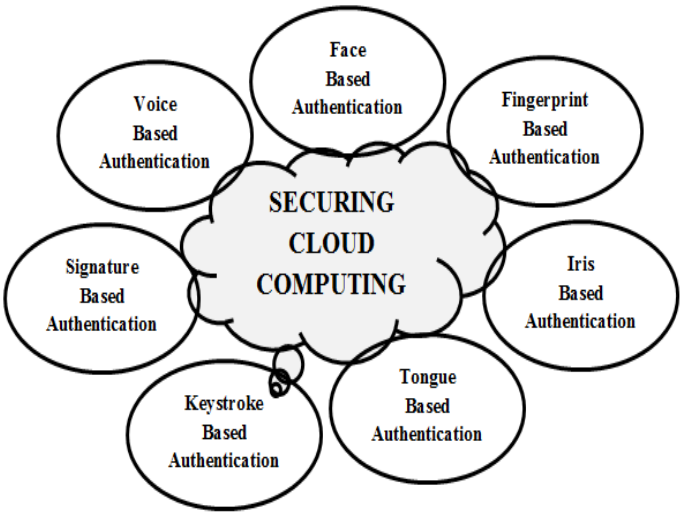

Fig. 5 – Biometric Techniques to Secure Cloud Computing

A. *Face Based Authentication*

Facial recognition (or face recognition) is a type of biometric software application that can identify a specific individual in a digital image by analyzing and comparing patterns [6]. These system mostly used for security purposes as well as used of these system rapidly increasing in other application areas.

- Related Work

Deepak S and Sai Goutham N [7] proposed face authentication or recognition system for securing mobile cloud. They have given five stages. These are: a) Registration of User: In this stage user will download mobile application. Then he will fill details with name and mail box ID. Mail box ID is authenticated. Entered data or information is stored in local cloud for further use. b) Face Capture: In this stage user will touch the mobile screen. Then mobile camera will be switched on. Mobile camera will capture face of user. c) Face Detection and Face Recognition: After capturing image, in this stage face will be identified from the captured image. Then face will be recognized by extracting features. Users face will be matched with face which is stored in database. d) Cloud Transfer: After matching face, image will be transferred to another cloud. Then after receiving image again it is transferred to user registered mail box ID. e) Screen Recording: In this stage recording starts after user activates application. It will record screen till application is deactivated. After deactivating application recording will stop. Recorded files will be stored in local memory.

B. *Fingerprint Based Authentication*

For century, humans are using finger prints for personal identification and access control. Fingerprint is made of a series of ridges and grooves on the palmar surface of the fingers [8]. Accuracy of finger print authentication has shown very high figure. Finger prints of twins are also different so it increases rate of accuracy.

- Related Work

Samadhan Pagar, Vaibhav Gore, Darshan Sant and Pooja Satpute [9] proposed a multi-user authentication scheme based on cellular automata by using thumb authentication. In this scheme thumb is used as authentication for securing cloud computing. Here whole data is stored by user along with the thumb image as security. The same user can download data with same thumb image to any other computer. Authors have proposed system for it. First thumb registration is done by user to facilitate under admin of system. After registering user will get thumb log in ID. To get login on system user can use thumb scan and get ID. On the client side user can use thumb scan. It will generate user's registered ID automatically if user is valid. Then user will login. It will generate 0 ID if user is invalid for unregistered users. And it will not proceed. User has to make registration on cloud server when thumb authentication is successful. Then user will fill details on cloud to get user id and password. Now user can do log in for cloud after registration is successful on cloud.

Alaa Hussein Al-Hamami and Jalal Yousef AL-Juneidi [10] proposed multi finger biometric scheme. This scheme uses three finger templates of user's choice and allocates single digit number for each of these three fingers. It is uses during registration of user. Elliptical algorithm is used to encrypt recorded images and it is stored at service provider's end. Encryption algorithm is applied at three levels. a) Finger Print Images, b) Three Single Digit Numbers and c) Mapping of these Three to the Images.

IehabALRassan and HananAlShaher [11] proposed fingerprint recognition system with mobile phone camera method. This method deals with how finger print recognition is used to secure mobile could is explained. Now a day there is very less work about using digital camera or web camera as sensor. To add separate fingerprint scanner or hardware will be very costly. So proposed system is used to get fingerprint image, through mobile camera for using finger print recognition system. In this method, first phase is enrolment phase. In this phase user provides fingertip to mobile phone camera. Then camera obtains fingerprint sample and extracted features by preprocessing sample. Then to verify user's identity, it is stored in database for further comparison. Fingerprint image is given as input on login form. The preprocessing image function is used to extract features. Then matching function is used to match between these features with features stored in database. User is accepted if matching is successful otherwise user is rejected.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

C. Iris Based Authentication

Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye [12]. Mostly, as like face recognition, Iris recognition is often used for security related applications such as in airports, government buildings for entry or exit. Iris recognition technology is more accurate as compared to other biometric techniques.

- Related Work

D. Kesavaraja, D. Sasireka and D. Jeyabharathi [13] proposed Cloud Iris Verification system (CIVS). CIVS system is having five steps, Segmentation, Normalization, Enhancement, Feature Extraction, and Storing / Verification. First an eye image is obtained from a B/W CCD camera. Detect only iris region from an eye image and to get segmented iris, for that author uses canny edge detection, thresholding, and circular hough transform methods. Now normalization performs on segmented image to get proper iris image. Histogram stretching method is used for enhancement. Cumulative sum based analysis method used by authors to extract features from iris images and for verification purpose hamming distance method is used. Authors were tested CIVS server against webs servers with password security. From the analysis result it has been found that CIVS Server stands unique in providing secure service to the user compared to the other web servers.

Nikhil Kumar, Dr. Yogesh Awasthi and Prof (Dr.) R. P. Agarwal [14] proposed fusion of fingerprint and iris biometric techniques to secure mobile cloud computing. In this model, when user login through fingerprint then binary code is generated. This generated binary code is stored in databases of service provider. Binary code is generated by the user hand, whenever user logins through fingerprint, which will be compared with stored binary code. If comparison result is true then user will get successful login. But authors said fingerprint will have low priority login process. So, they also proposed high priority login process by using iris biometric technique. At the time of account created with cloud, in that first need to complete enrollment process. In that, scan the iris by eye scanner. Then generated iris code will be stored in the database for matching. In recognition process, registered iris code and scanned iris code are compared using hamming distance. If matched then user successful login else access is denied. So, only authorized user can access the cloud.

D. Tongue Based Authentication

The tongue is unique to each person in its shape and in its surface textures [15]. Tongue is an internal organ but it can be easily used for authentication. Tongue consists of seams, ridges and wrinkles. These are unique. As like eyes or fingerprints, tongue can't be used without the person's consent.

- Related Work

Sowmya Suryadevara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anand Sharma [16] proposed PCA based tongue recognition system for security. In this paper authors have divided their system into three parts i.e. User, Cloud Initialization and Private Matching Identification. In user part paillier encryption method is used for preprocessing of original image of tongue. Cloud initialization part deals with processing original image and to create subspaces as well as tongue template database through PCA algorithm. Private matching identification part is used to project, distance calculation and minimum distance finding purpose.

E. Keystroke Based Authentication

Keystroke dynamics is based on the habitual rhythm patterns in the way a person types [17]. It contains speed, time required between specific key, routine errors and the time required of that keys are released.

- Related Work

Mahnoush Babaeizadeh, Majid Bakhtiari, and Mohd Aizaini Maarof [18] proposed a multi-factor authentication method for mobile users in cloud environment to identify users. In this, first factor is username/password and second is keystrokes authentication. Steps to perform authentication: a) Login by valid username/password, b) application calculate the duration of keystroke, v) calculated duration will be encrypted by using Trusted Third Partner (TTP), and d) finally, all the values (username, password, keystrokes duration) will send to Cloud Service Provider (CSP). This technique doesn't require any extra special tool therefore it is cheaper than other type of biometric authentication methods.

F. Voice Based Authentication

Voice recognition systems use characteristics of the voice like pitch, tone, frequency, etc. [19]. It is also called as speech recognition system. This technique is focuses on the differences of vocal tracts and learned speaking habits. This technology is less costly, easy to use and non-intrusive. Due to poor environment, it can create problem, also has low accuracy.

- Related Work

R. Gokulavanan and Dr. N. Shanthi [20] proposed Single Sign-On framework using OpenID model with voice biometric technique. OpenID is a Single Sign-On protocol. Because OpenID, there is no need to used separate login and password for every website. For that, first, it is necessary to register with an Identity Provider (IdP) then use same login to all OpedID enabled sites. As OpenID is a decentralized system. Once the user is successfully authenticated by identity provider, then identity provider gives unique URL for user. Now, to exchange the data, an IdP and a Relying party (RP) shared cryptographic key. IdP and RP use the Diffie-Hellman (DH) algorithm. Now the user is redirecting to the IdP

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

server, they log in and authorize the Relying Party. Once login is performed into one site, they can be automatically logged into other sites.

K. Marimuthu, D. Ganesh Gopal, Harshita Mehta, Aditya Rajan and P. Boominathan [21] proposed method to solve drawbacks of One Time Password (OTP) to prevent phishing attacks. They integrate voice biometric technique with one time password method. This solution contains two process namely, registration process and login process. To complete registration process, user needs to provide required details. Then perform CAPTCHA test to distinguish humans and computers. By using random function, unique username is generated. Now, need to supply voice password. Once the voice password is confirmed then all user's details along with voice password is stored on the cloud. Finally, confirmation message is sent through an email. For login process, user needs to provide unique user Id. Once the user Id is verified then OTP is generated, stored on the cloud and also send to user through email. Once the user provides the OTP, then it compared to the cloud OTP. After the OTP is verified the user is need to provide the voice password. Again this voice password is compared to the voice password stored on the cloud. If matches the user can successfully login.

G. *Signature Based Authentication*

Signature recognition is used to authenticate user's identity based on the traits of their unique signature. It is a behavioral characteristic of human. It may change during a period of time.

- Related Work

Hongwei Li, Yuanshun Dai and Bo Yang [22] proposed a Hierarchical Architecture for Cloud Computing (HACC), Identity-Based Encryption (IBE) and Identity-Based Signature (IBS). Finally, an Authentication Protocol for Cloud Computing (APCC) is constructed based on HACC, IBE and IBS. The HACC is consists of three levels. The top level is root Private Key Generator (PKG). The middle level is sub-PKGs. Each node in middle associates to a cloud storage service provider. The bottom level are users in the cloud computing. The main tasks of the IBE are encryption and decryption as well as main tasks of the IBS is signature and verification. APCC uses the RSA key exchange algorithm. In the APCC, the computation cost of client is one IBE encryption and one IBS signature as well as for server is one IBE decryption and one IBS signature verification, as well as the communication cost is only one IBS signature and one IBE cipher text as compared to SSL Authentication Protocol (SAP). Author performed simulation experiments on GridSim which is based on Java, it was shows that the authentication protocol is more lightweight and efficient than SAP.

V. COMPARTIVE STUDY OF EXISITNG BIOMETRIC TECHNIQUES IN CLOUD COMPUTING

Table II shows an overview of different biometric techniques proposed for secure cloud computing by different authors and its advantages:

Table II. Proposed biometric techniques to secure cloud computing

SN	Type of Biometric Technique	Name of the Paper	Author(s)	Proposed Method / Technique / Model / Scheme	Advantage(s)
1	Face	Face Recognition using Cloud Based Security in Mobile Devices	Deepak S and Sai Goutham N	Face authentication or recognition system for securing mobile cloud	The proposed system is easy to use and easy to implement
2	Fingerprint	The Thumb Authentication on Cloud Computing	Samadhan Pagar, Vaibhav Gore, Darshan Sant and Pooja Satpute	A multi-user authentication scheme based on cellular automata	The proposed scheme was lightweight, secure and robust. The randomness quality is high
3	Fingerprint	Secure Mobile Cloud Computing Based-On Fingerprint	Alaa Hussein Al-Hamami and Jalal Yousef AL-Juneidi	Multi finger biometric scheme	The proposed scheme is simple and gives user multiple options for login
4	Fingerprint	Securing Mobile Cloud Using Finger Print Authentication	IehabALRassan and HananAlShaher	Fingerprint recognition system with mobile phone camera	The proposed method is not only secure but also to protect from injection attacks
5	Iris	Cloud Software as a Service with Iris Authentic	D. Kesavaraja, D. Sasireka and D. Jeyabharathi	Cloud Iris Verification System (CIVS)	The proposed system is relatively simple and secure

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

6	Iris	Authenticating Cloud & Data Center with Iris	Nikhil Kumar, Dr. Yogesh Awasthi and Prof (Dr.) R. P. Agarwal	Fusion of biometric authentication techniques (Fingerprint and Iris)	The proposed technique is highly reliable and secure
7	Tongue	Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security	Sowmya Suryadevara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anand Sharma	PCA algorithm for tongue recognition	The proposed method guaranties to be credible, efficient and low-complex
8	Keystroke	Authentication Method through Keystrokes Measurement of Mobile users in Cloud Environment	Mahnoush Babaeizadeh, Majid Bakhtiari, and Mohd Aizaini Maarof	Multi-factor authentication method	The proposed method is improved the security and privacy
9	Voice	Cloud User Voice Authentication enabled with Single Sign-On framework using OpenID	R. Gokulavanan and Dr. N. Shanthi	OpenID protocol with voice biometric authentication technique	The proposed technique provides seamless and transparent login process
10	Voice	A Novel Way of Integrating Voice Recognition and One Time Passwords to Prevent Password Phishing Attacks	K. Marimuthu, D. Ganesh Gopal, Harshita Mehta, Aditya Rajan and P. Boominathan	Voice password with One Time Password (OTP)	The proposed method is highly secure and robust as well as increases effectiveness
11	Signature	Identity-Based Cryptography for Cloud Security	Hongwei Li, Yuanshun Dai and Bo Yang	IBE and IBS for HACC with an APCC	The proposed method achieves great scalability

VI. CONCLUSION

Cloud computing is mostly based on two concepts, first is sharing and second is pay for use. Cloud computing provides variety of services like Iaas, SaaS, and PaaS. So, it is very important to allow only authorized users to access these rendered services in cloud. To provide cloud services only to the authorized user, secure authentication is necessary in cloud computing. There are so many traditional authentication techniques available like password, OTP etc. but still it has some drawbacks like at times password techniques are not feasible, password can be easily stolen by hacker or if user uses complex password, user may forget that password etc. So it is a better option to use biometric authentication techniques rather than traditional authentication techniques. The security level of cloud provider in terms of secure authentication is much improved by using biometric authentication system. This paper contains various biometric authentication techniques which are proposed by different authors for cloud computing environment. We elaborately examine all these proposed methods. From our observation, we conclude that the biometric authentication techniques give novel solutions to authenticate user in cloud computing. Also, it offers a good foundation for further research for providing security in cloud computing.

REFERENCES

[1] NIST Special Publication 800-145, "The NIST Definition Cloud Computing"

[2] Shivashish Ratnam, Mimzee Gupta, Dr. Ajay S. Singh and Thirunavukkarasu K, "A Survey on Biometric Security Technologies from Cloud Computing Perspective", International Journal of Scientific and Technology Research, ISSN: 2277-8616, Vol. 5, Issue 4, April 2016

[3] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

[4] "The Treacherous 12 - Cloud Computing Top Threats In 2016", February 2016, [Online] Available: Https://Downloads.Cloudsecurityalliance.Org/Assets/Research/Top-Threats/Treacherous-12_Cloud-Computing_Top-Threats.Pdf. [Accessed 25 November 2016]

[5] Jammi Ashok, Vaka Shivashankar and P.V.G.S. Mudiraj, "An Overview of Biometrics", International Journal on Computer Science and Engineering (IJCSE), ISSN: 2402-2408, Vol. 2, No. 7, 2010

[6] Ananya Dua and Anikesh, "Incentive for Using Face Recognition, The Applications of This Technology", International Journal of Science, Technology & Management, ISSN (online): 2394-1537, Vol. 3, Issue No. 4, April 2014

[7] Deepak S and Sai Goutham N, "Face Recognition using Cloud Based Security in Mobile Devices", International Journal of Innovative Research in Computer and Communication Engineering, (An ISO 3297: 2007 Certified Organization), ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 3, Issue 6, June 2015

[8] Nagy M. B. Al-Fadaly, "Potential Role of Knee Print in Forensic Identification", J Forensic Res, ISSN: 2157-7145 JFR, Vol. 2, Issue 5, 1000131

[9] Samadhan Pagar, Vaibhav Gore, Darshan Sant and Pooja Satpute, "The Thumb Authentication on Cloud Computing", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 5, May – 2014

[10] Alaa Hussein Al-Hamami and Jalal Yousef AL-Juneidi, "Secure Mobile Cloud Computing Based-On Fingerprint", World of Computer Science and Information Technology Journal (WCSIT), ISSN: 2221-0741, Vol. 5, No. 2, 23-27, 2015

[11] IehabALRassan and HananAlShaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications (IJNSA), Vol. 5, No. 6, November 2013.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

[12] Anushree S. Patil and Prof. S. M. Rajbhoj, "Embedded Systems for Iris Recognition", International Journal Of Engineering Sciences & Research Technology (IJESRT), ISSN: 2277-9655, February 2016

[13] D. Kesavaraja, D. Sasireka and D. Jeyabharathi, "Cloud Software as a Service with Iris Authentic", Journal of Global Research in Computer Science (JGRCS), ISSN: 2229-371X, Vol. 1, No. 2, September 2010

[14] Nikhil Kumar, Dr. Yogesh Awasthi and Prof (Dr.) R. P. Agarwal, "Authenticating Cloud & Data Center with Iris", International Journal of Engineering and Technical Research (IJETR), ISSN: 2321-0869 (O) 2454-4698 (P), Vol. 4, Issue 3, March 2016

[15] Manoj Diwakar and Manish Maharshi, "An Extraction and Recognition of Tongue-Print Images for Biometrics Authentication System", International Journal of Computer Applications, ISSN: 0975–8887, Vol. 61, No. 3, January 2013

[16] Sowmya Suryadevara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anand Sharma, "Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security", International Conference on Information and Network Technology, IPCSIT Vol. 4, 2011, IACSIT Press, Singapore

[17] Moitrei Bharadwaj, Amreesha Kakati, Ankita Bharali and Aniruddha Deka, "A Keystroke Dynamics Based Authentication System", Journal of Basic and Applied Engineering Research, p-ISSN: 2350-0077, e-ISSN: 2350-0255, Vol. 2, Issue 20, October-December 2015, pp. 1745-1748

[18] Mahnoush Babaeizadeh, Majid Bakhtiari, and Mohd Aizaini Maarof, "Authentication Method through Keystrokes Measurement of Mobile users in Cloud Environment", Int. J. Advance Soft Compu. Appl, Vol. 6, No. 3, November 2014 ISSN 2074-8523

[19] Harpreet Saini and Kanwal Garg, "Comparative Analysis of Various Biometric Techniques for Database Security", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Vol. 2, Issue 4, April 2013

[20] R. Gokulavanan and Dr. N. Shanthi, "Cloud User Voice Authentication enabled with Single Sign-On framework using OpenID", International Journal of Innovations in Engineering and Technology (IJIET), ISSN: 2319–1058, Vol. 4, Issue 1, June 2014

[21] K Marimuthu, D Ganesh Gopal, Harshita Mehta, Aditya Rajan and P BoominathanTavel, "A Novel Way of Integrating Voice Recognition and One Time Passwords to Prevent Password Phishing Attacks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.5, No.4, July 2014

[22] Hongwei Li, Yuanshun Dai and Bo Yang, "Identity-Based Cryptography for Cloud Security"