Biometric-based Authentication Techniques for Securing Cloud Computing Data - A Survey

Asmaa M. Hussein
M. C. S. Scholar
Helwan University, Cairo, Egypt

Hala M. Abbas
Assist Prof, Computer science dept., faculty of computers & information, Helwan University, Cairo, Egypt

Mostafa-Sami M. Mostafa
Prof, Computer science dept., faculty of computers & information, Helwan University, Cairo, Egypt

ABSTRACT
Cloud Computing is the most growing paradigm for delivering computational resources as a service over the internet. By 2018, many different enterprises have adopted this utility-based computing for reducing the operational and capital expenditure of building their infrastructure network, buying software licenses, hiring IT teams and other requirements. With this unlimited growth of using cloud services and the multi-tenancy nature of sharing cloud service instance between different consumers and enterprises, securing accessing to the data of the cloud became a major issue. Traditional authentication techniques and credentials does not provide enough security against the modern means of attacks. So, new biometric-based authentication techniques have been discovered to overcome the loop holes. Here we present a comprehensive survey on the existing user's authentication techniques especially biometric-based techniques used for accessing cloud data.

General Terms
Security, Human Factors, Performance.

Keywords
Cloud Computing, Cloud Security, User authentication techniques, Biometric authentication.

1. INTRODUCTION
According to the National Institute of Standard and Technologies (NIST) [1][2] Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned, scaled up or down and released with minimal management effort or service provider interaction". Cloud showed up with five main characteristics [1][3]: On-demand self-service where users can reach cloud resources without a human interaction, Ubiquitous/Broad network access where users can get access to cloud resources over a wide range of devices such as PCs, laptops, and mobile devices, Location Independence, resources can be physically located at many geographic locations and assigned as virtual components when needed, Rapid elasticity is the ability provided for users to scale up or down their used resources quickly and efficiently and Measured service, where users bay only for what they use.

Cloud is gaining a high attention of providing different kinds of service models, allowing users to choose the appropriate service delivery model that fits their needs of different storage spaces, processing power, productive applications, networking equipment provided in different packages as [4]: Software as a Service (SaaS) for users who only need to use the provider's applications with no control on the network, servers, OS, storage or applications like Apple's MobileMe, Google Apps [5], Salesforce.com [6]. Platform as a Service (PaaS) provides users with programming languages, libraries, services, and tools to deploy their own created applications supported by the provider as Google App Engine [7], force.com, Microsoft Azure [8]. Users of this service can't control the underlying cloud infrastructure. Infrastructure as a Service (IaaS) makes users getting access to the fundamental resources of cloud like OS, storage, and possibly limited control of network components to deploy their stuff but no control on the underlying cloud infrastructure as Amazon EC2 [9] and S3 [10], Sun Microsystems Cloud Services or Dropbox [11].

When using the cloud model, end-users don't aware where data is stored and how it is being processed, they only can get access to it. Controlling and securing access processes to cloud data needs using strong authentication techniques as attackers target the techniques that users pass through for accessing their data. The authentication process is a simple function of some credentials for a system to verify specific information presented from a genuine access of the system. Authentication is a significant element of cloud, securing environment. It is classified into three categories depending on security levels [12][13]: Knowledge-based authentication techniques, Possession-based authentication techniques and Biometric-based authentication techniques as will be described next.

2. CLOUD AUTHENTICATION TECHNIQUES
When a user tries to access his data, a management module for authentication, authorization and accounting (AAA) checks the user's authentication information. Authentication process determine "Who is the legal user?" and "Is the user really who claims himself to be?" using one of the next techniques [14]:

2.1 Knowledge-based Authentication Techniques
Is the simplest of all authentication techniques which based on owning some information exclusive to the user. Something user knows and is characterized by secrecy, such as username and password, security question, personal identification numbers (PIN) based authentication scheme and Implicit Password Authentication System (IPAS) [12] [13]. Username and Password Authentication- is the most commonly used technique. Most users pick something easy to implement, easy to memorize from their daily life, and requires no special equipment as their telephone number, birth date or some related names. Users might share their password with other which make it so easy for attackers to discover.

Gurav et al. [15] proposed a graphical password authentication model for improving the security of Cloud. They presented an identification algorithm based on the selection of username and images as a password. Thus, graphical password authentication can be given by taking cloud as a platform. According to psychological studies human mind easily remember images than alphabets or digits.

To make the password more difficult for discovering, strong password must have a combination of numbers, letters, and special characters [16]. But, this didn't prevent attacks from a special kind of attacks as: Brute force attacks: where attackers try to crack the encrypted passwords, Dictionary attacks: where attackers try to match the user password with most occurring words or words of daily life usage [17], Phishing attacks: are a web-based attacks in which the attacker redirects the user to the fake website to get passwords/Pin Codes of the user [17], Shoulder surfing attacks: in which the attacker observes the user's movements of how he enters the password and what keys are pressed, Replay Attacks: known as the reflection attacks. It is a way to attack challenge response user authentication mechanism, or key logging attacks: the software programs which monitors the user activities, by recording each key pressed by the user [17] [18].

Knowledge-based authentication techniques suffer from well-known limitations [19]. Furthermore, it is difficult to confirm that the demand authentication data is from the rightful owner with just matching the letters of the password [20]. Password is a single factor authentication technique if used alone and can be merged with other techniques to perform multi-factor authentication techniques as will be declared next.

2.2 Possession-based Authentication Techniques

The Possession-based authentication techniques are the second kind of authentication techniques which is based on something the user has. such as a security electronic token, a key, trusted device, passport, smart cards, or ID card as an Automatic Teller Machine card (ATM card) [21] [22]. Those physical devices were developed to overcome certain weakness associated with using passwords. They can also be used lonely or with passwords and other techniques. A user sends his username and password as the first factor to the Cloud server for authentication. When user's a username/password matches with a Cloud server's database, the Cloud server asks the user to send his second factor's credentials as electronic token or a card as we early explained (see Figure 1). When the user's second factor has validity in the Cloud server, the user gains permit to reach a Cloud server's resources [23].

Fig 1: Principle of 2FA in cloud computing [23].

Chen [24] and Choudhury [25] used smart cards and USB for making the system more secure in authentication. Where secret keys and credentials stored on a USB and smart cards provided from service providers. These devices help to perform a good level of authentication, but they might be lost or stolen easily. Also, Nayak et al. in [26] proposed an authentication scheme for cloud service users using symmetric keys to secure the communication between user and server. If the ID and password match, the server generates a dynamic token to user's email to complete the authentication process. This scheme requires the user to log into two accounts during the authentication process which may cause user inconvenience.

In 2012, a hacker group named UGNazi "*underground nazi*" hacked the Gmail account of the Cloudflare's CEO "*Chief Executive Officer*" by sneaking into a significant flaw in the Google's password recovery system. UGNazi sent an account recovery request to his phone, which was forwarded to their number, and then used it to take over the personal Gmail [27]. Once they were in, they used it to get into the corporate Email by doing an account recovery. The hacker easily bypasses the two-factor authentication mechanism of Cloudflare and had access to the Cloud account of the victim. Since the victim was the CEO of Cloudflare, the hacker had the administrative privileges and changed the passwords of several other accounts. Cloudflare immediately blocked the account and reset the password of all the accounts. Google then re-worked on its password recovery mechanism to make it not possible to by-pass the two-factor authentication module [27]. Google spokesperson gave Wired a statement noting "We fixed a flaw that existed in the account recovery process for Google Apps for Business customers under very specific conditions" [28].

Possession-based systems have the advantage of not being able to be shared with others, but, they are not effective for users that do not remove their token when leaving the system unattended. Besides, a stolen token would give an attacker the same access rights as the genuine user and could not be detected by the computer system [29]. The card readers used to consider an additional cost and requires extra application to acquire a match between smart card and correspondence models. And, it may be lost or broken with card theft.

2.3 Biometric-based Authentication Techniques

Biometric technique is based on something user is. It uses the measurements of physical characteristics or personal traits to validate the subject identity. The permanent ownership of human has increased the chances of deploying biometric-based authentication in highly secure systems. Human characteristics cannot be shared and not duplicable or transferable with others [30], so it easily allows systems to keep track of human activities. Usual authentication techniques can't confirm the identification of the real ownerm but using the unique characteristics of human resolve that problem. Biometric is an automated method for easily verifying and recognizing the identity of a living person based on his physiological or behavioral characteristics. It is an excellent candidate for providing an extra level of security, especially when used in conjunction with traditional methods for authentication [13].

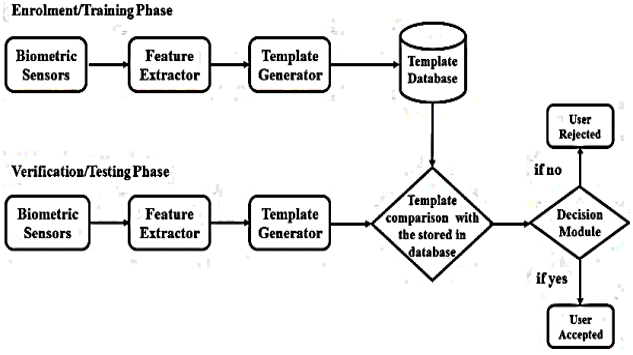

Fig 2: General design for biometric-based system [31] [32].

Generally, biometric-based authentication systems consist of two phases (see Figure 2). In the Enrollment Phase, raw data is collected from participants via different kinds of input devices with sensors. Those sensors depend on a kind of biometric used for the authentication. They scan and capture the user's basic data through training sessions on the system. After extracting the features of the scanned biometric using an algorithm, a feature vector used for generating a template for each user. This template is encrypted using the public key obtained from a Cloud server then send back to it to be stored in the template database for later use. With the growth of cloud, it is the time to offload heavy loads to cloud.

In the verification phase, the biometric sensor, the feature extractor and generator, perform the same tasks as in the enrollment phase. However, the template generated will not be stored in the Cloud. Instead, it will be compared with the previously stored template by using a classification or regression algorithm [33]. For the matching step, different classifiers can be used as statistical approaches, ANN, SVM, Manhattan Distance, Euclidean Distance and K-mean. The decision module is responsible for making the final decision based on a threshold previously determined by the system administrator. If any match occurs, the user is accepted and authorized to use the Cloud service otherwise an error message is sent for the user for relogging again [34]. After unsuccessful specified number of login attempts, an Alternate Verification Code is mailed to the user's registered Email address if exist or the user is rejected, and the account is locked [35].

In this phase, the performances of the keystroke biometric systems are measured based on three kinds of metrics that estimate the accuracy of classifications and regression algorithm used [36] [37]: The first metric is called False Acceptance Rate (FAR) which is the rate at which a biometric system accepts a sample of an impostor pretending as a valid user and trying to successfully gain access to a secured system. It is also known as Type II error [13]. The second metric is called False Rejection Rate (FRR) which is the rate at which a biometric system incorrectly rejects a sample provided by the valid user. It is also known as Type I error. Equal Error Rate (EER) is the point where both FRR and FAR have an equal rate value when one increases, the other decreases. Sometimes it called Cross Over Error Rate (CER). System with lower EER/CER provide the best performance [13]. The accuracy of authentication is evaluated using the equal error rate (EER) on the Receiver operating characteristic (ROC) curve [38].

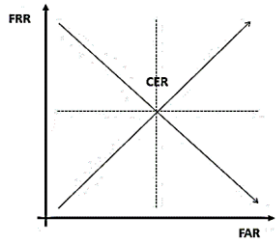

Fig 3: ROC curve of CER [39].

Wong, et al. [33] propose a biometric-based authentication protocol as a second factor for cloud user's authentication using biometric traits of the user and a verification code. They achieved secure authentication for cloud while protecting the sensitive information of users. Biometric authentication techniques are broadly classified in two categories: physical and behavioral biometric characteristics (see Figure 4) [22]:

1- *Physiological biometrics* perform authentication based on bodily characteristics and shape such as Fingerprint, Face, Iris, Retina, Hand Geometry, Palm Vein, DNA, skin reflectance, odor, and ear shape.

2- *Behavioral biometrics* which is based on the way people do things, such as voice, signature, keystroke dynamics, gait, mouse dynamics and lip motion.

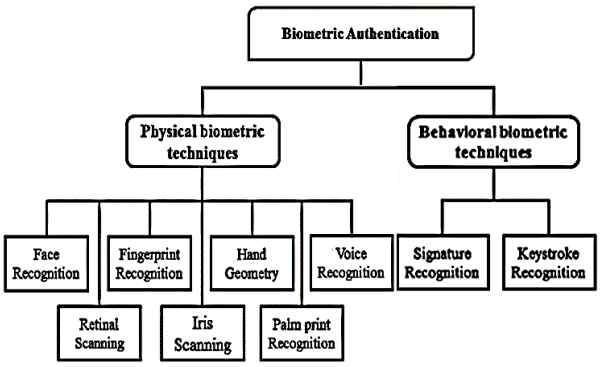

Fig 4: User Authentication Classifications [13].

2.3.1 Physiological Biometrics Techniques

Physiological characteristics based on direct action of physical parameters of a certain part of the body and they are unalterable without causing trauma to the individual. Physiological characteristics identify users based on their Face Recognition, Fingerprints Recognition, Hand-Geometry, Voice Scanning, Retina Scanning patterns, Iris Scanning, Palm-Print etc.

2.3.1.1 Face Recognition

Face Recognition is a popular biometric technique where facial recognition features are different from one person to another. The system automatically takes a 3-dimensional digital image or a video frame of the face, extracting 3-dimensional facial features such as the shape of the eyes (eye brows and eye areas (ocular) size), nose, cheekbones and jaw from that image, then saves it in the database [40]. In verification procedure the facial features being extracted are matched by the already stored template using a match engine. Atmakuri, et al. [41] proposed a new biometric-based authentication framework using face technique where the facial features extracted from user's mobile device. For access the cloud, user needs first to give his email id as his user name to be checked in the database. Then, an image of the user's face is taken, extracting the facial features using the Geometric approach and matching with the stored template in database. Face Recognition is a cheap technology. It gives a quick identification response. But, it faces a major problem where faces are a social part and its expressions are changed [42].

2.3.1.2 Fingerprint Recognition

Fingerprint recognition is the oldest highly acceptable recognition type of all the biometric-based techniques. In which no individuals share same finger prints even if they were twins. The old traditional method used the ink to get the fingerprint onto a piece of paper and scan it on a traditional scanner. But now in modern approach, live fingerprint sensors are used based on optical, thermal, silicon or ultrasonic principles [43]. Whenever a finger is placed, sensors scan the image of the finger. The fingerprint patterns are identified

using sub-characteristics such as crossover, core, bifurcation, ridge ending, island, delta, pores etc. [44]. Image and password both are stored in the CSV database for later matching process. If the password and the image matched, then the user can be allowed to use the desired service [45].

ALRassan, et al. [46] implement a new authentication technique of mobile cloud using fingerprint recognition system to secure accessing mobile cloud resources from illegitimate users. They used the mobile device camera as a fingerprint sensor to obtain a fingerprint image for processing. Sabri, et al. [47] enhance the security performance in cloud by eliminating the concerns of data security using bio-hash function to secure the stored fingerprint biometric templates. They used a well know benchmark CASIA fingerprint-V5 data sets. Biometric technique is a multi-factor authentication technique, it can be used separately or with other authentication techniques to provide a multi-factor authentication system. Venakatesan, et al. [48] created a multi-factor biometric-based authentication system. They used the finger print recognition technology with the id and the password of the user to overcome the security serious issues in systems implementing biometrics-based authentication. Finger print recognition system is the most used biometric system nowadays. It has the advantage that the arrangement of the rims and structures do not change during the lifespan of the human but, if there is any noteworthy injury that crafts an everlasting scratch or users has intensive laborers, there will problems [49]. Plus, some aspects of skin surface such as dryness, wetness can significantly affect the quality of the image in the matching process. Also Finger print recognition system is expensive to be used easily [50].

2.3.1.3 Iris Scanning

Iris is a circular part surrounding the pupil in the human eye controlling the eye from the light entering. Iris recognition technique used to recognize human's unique arrangements. Iris features are very recognizable and unique for each human [51]. In this mechanism, an image of the eye is taken using a high resolution digital camera to be analyzed by the infrared or visible waves [52]. Then features like striations, pits and furrows are extracted and stored in cloud database. In the verification phase, a special algorithm is used to check whether the image matches the stored one or not. Iris should not be farther than a few meters from the camera and must be stationary to get an accurate result [41]. Abduljabbar, et al. [53] proposed a robust non-interactive one-time biometric key which is used to generate one-time cloud login request message. This key has two strong building blocks; it is biometrically based on the extraction of features from the entities' irises, and cryptographically based on the strong key-based message authentication code MAC-SHA-512 and Rivest Cipher 4. The major drawback that Iris identification cannot be applied universally for people suffering from severe eye illness and visually challenged. It also needs special equipment for scanning, which has a high-resolution capacity.

2.3.1.4 Retinal Scanning

The retina is a unique thin tissue composed of neural cells located in the posterior part of human eyes. Verification of user identity done through the images of blood vessels in the eye using infrared illumination. Characteristics extracted from retinal scanning are outer iris, pupil edge, blood vessels. The major drawback of this technique as Iris scanning, it cannot be recognized for people suffering from severe eye illness and visually challenged people [54]. And, it is highly cost so, it used in military installations [31].

2.3.1.5 Hand Geometry/Recognition

Although hand geometry cannot provide performance as some other biometric features, it is still a good choice for personal identification because of its simplicity, low-cost and high user acceptance properties. It is a process in which the system sensor extracts a unique geometric feature of the hand, such as the length of the fingers, width of hands, finger thickness, distance between finger joints and hand's overall bone structure [41]. Image acquisition system is composed of commercial webcam, InfraRed (IR) filter, and some sets of doubles- rows GaAs infrared emitting diode. Users can place their hands free in front of the camera. Some processing steps are applied to solve the problems arising in the feature extraction process which makes it possible for users to flexibly place their hands with arbitrary orientations [55]. Aumi and Kratz [56], use in-air hand gestures to authenticate users tracked through a short-range depth sensor. They track multiple distinct points on the user's hand simultaneously

2.3.1.6 Palm Vein Recognition

Palm Vein Recognition is a recent authentication technique in which Vein patterns rely on the biological information of the interior body which is a vast network of blood vessels underneath the person's skin. Those vessels are barely visible to the human eye; therefore, it is not easy for intruders to get information about. The verification is done using palm prints in hand like a finger print. The image of hand palm is taken with spread fingers by the sensor. Then image goes from various processing for the features of the image to be extracted and form a template. This template is used for matching features with new registered image. If matching is completed successfully the user can access services from the cloud. Ziyad, et al. [57] proposed a multifactor biometric-based authentication of using the fingerprint, palm vein, traditional smart card, and user password. Authors handle the biometric data in a secure fashion by storing the palm vein data in multi-component smart cards and fingerprint data in the central database of cloud security server. For security enhancing, the phase of biometric data matching is performed on the card with Match-on- Card technology and data never leave the smart card. Palm prints considered unique and are found to be better than finger prints in recognizing prints with burns, oil stains, cuts etc. [36]. It cannot be easily damaged, changed or falsified.

2.3.2 Behavioral Biometric technique

Behavioral characteristics are related to what a person does, or how the person uses the body. It can identify users based on their location or unique behavioral characteristics such as the pitch and amplitude in their voice, the way they sign their names, and even the way they type "keystroke dynamics", form the basis of non-static biometric systems. Two important types of behavior biometrics are Voice, Signature Recognition and Keystroke Dynamics.

2.3.2.1 Voice Recognition

Voice recognition technique does not require any costly devices. The recognition is done by recognizing the speaker's voice frequency, nasal tone, cadence, inflection etc. based on a multitude of parameters that can prevent mimicking of the one's voice by another person. The drawback is that the voice of the individual can change with age, illness, mental state. Moreover, recorded voice can also have played to bypass the system [54]. Baloul et al. [58] proposed a free text speaker recognition method to guarantee the security of electronic transactions from the replay attacks.

2.3.2.2 *Signature Recognition*

The signature recognition technique has been used for a long time for verification purposes. Older methods depend on manual signatures, but nowadays signatures are getting digitized using a digital tablet with a pen provided to work as a sensor. Signature verification technology tests the behavioral features of typing as stroke order, formation of letters, speed, pressure, angle of writing and other traits [59] [60]. The verification phase is based on static or dynamic signature. In the static signature, the images of the sign are analyzed, so the user needs to duplicate the sign to authenticate. This way gives the ability for forgery as cyber criminals can easily replicate a sign to look like that of an image [61]. In dynamic signature, features as velocity, angle, position and orientation of certain points, curved lines in the signature, or underlined alphabets, etc. are extracted from the origin data for future comparison against every set stored in the database of CSP. A matching score is generated for deciding whether to accept the individual as identified user or not [49]. Dynamic signature is more comprehensive and more reliable than Static as it involves more behavioral traits, but change under the influences of illness, Emotion etc. [62]. Yassin, et al. [61] proposes a two-factor authentication scheme based on Schnorr digital signature and fingerprint features to overcome cloud security issues. Their scheme fights different malicious attacks as off-line attack, dictionary attack, parallel-session attack, MITM attack, insider attack, and replay attack.

2.3.2.3 Keystroke Dynamics

The origins of keystroke date back over 150 years to the invention of the telegraph used in military applications, in which a person can be identified by the "fist" or rhythm of dots and dashes "Morse code" [63]. Keystroke dynamics is the process of analyzing the habitual rhythm of a user typing on a keyboard or on a mobile touch screen device to extract typing features as speed, latency between keystrokes, and pressure [64]. Those features are used to create a unique signature for each user "No two users type in the same way [65]" for easily later identifying. A classifications or regression algorithm such as Pattern Recognition, Neural Networks or Machine Learning is needed to be used to generate a template of features such as keystrokes timestamps of Dwell Time (DT) and Flight Time (FT) or key pressure, orientation [66]. The template of the user is stored in the database server on the cloud for future matching. New researches in 2017 identify some problems to take into considerations when designing a keystroke system and how to improve the accuracy of this system [21]. J Miya's method [67] achieved more than 96.5% accuracy. They used the keystroke recognition as a first factor of two-factors authentication system and use the password as the second factor for the.

2.3.2.4 Gait recognition

Gait is a new technique for user's authentication and still under development. It identifies people by analysis of the way they walk. It can be affected by terrain, injury, footwear, fatigue or personal idiosyncrasies [31]. Derawi et al. [68] propose a gait recognition system as a protection mechanism which is based on the use of video sources, floor sensors or dedicated high-grade accelerometers. They collect the dataset with a mobile device, and preprocessing, cycle detection and recognition-analysis were applied to the acceleration signal.

The following table will briefly discuss the advantages and disadvantages of Physiological Biometric techniques.

Table 1: Comparison of Physiological and Behavioral Biometric techniques used for Cloud Computing Authentication [31].

Method	Function mechanism	Advantages	Disadvantages
Face	Using 2-dimensional facial features such as Eye brows and eye areas	- Highly and simply accepted by users. - Good accuracy/low error rate	- Need additional hardware - As social part of people treatments, face expressions are being changed. So it is not much accurate
Finger-print	Based on optical, thermal, silicon or ultrasonic principles	- Good accuracy/low error rate - Used for over 10 years - No need for high power or cost	- Need additional hardware - Dirty or damaged fingers can affect the image of testing the accuracy
Iris	Using infrared or visible waves to process the image of unique arrangements in iris	- Very reliable with low error rate - Gives high results of accuracy	- High cost special equipment for scanning - Some people have phobia to expose eyes to light - Require long time for authenticating
Retina	Imaging of blood vessels in the eye using infrared illumination	- Very reliable with low error rate - Gives high results of accuracy	- High cost special equipment for scanning - Most people suffering from severe eye illness - Some people have phobia to expose eyes to light - Require long time for authenticating
Hand	Based fingers length and thickness, distance between finger joints and hand's overall bone structure	- Simplicity and low-cost, non-contact, high user acceptance properties	- Need additional large hardware for scanning - Hand geometry features are not very unique
Palm Vein	Rely on the interior vast network of blood vessels underneath the person's skin	- Gives high results of accuracy - Not easy to be changed or falsified.	- Need large expensive hardware for scanning - Detection equipment tool exposes transmission of many germs from different users
Voice	Rely on speaker's voice frequency, nasal tone, cadence, inflection	- Highly accepted and easy to use	- Doesn't work well with illness - Resaults are not very high accuracy

Signature	Typing features as stroke order, formation of letters, speed, pressure, angle of writing and other traits	- Highly accepted	- Results are not very high accuracy
Keystroke	Rely on typing features as timestamp, pressure and orientation	- Provide continuous authentication - No need for additional hardware	- Results accuracy are inconsistent
Gait	analysis of the way they walk	- Provide continuous authentication	- Results accuracy are low

In general, there are seven criteria to evaluate the suitability of biometric characteristics [69] - Table 2 as: *Universality:* the biometric solution can be used by everyone. *Uniqueness/ Distinctiveness:* difference in characteristics even between two people. *Performance*: the characteristics should give excellent speed and accuracy with minimum exploitation of resources. *Collectability*: the characteristic should be available in quantity. *Durability*: the characteristics should remain the same over the time. *Acceptability*: people should accept the use of characteristics in their daily life. *Circumvention*: represents how easily the system can be deceived.

Table 2: Comparison of Different Characteristics of Biometric Techniques (H: High, M: Medium, L: Low) [31] [36].

Biometric Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	H	M
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Hand	M	M	M	H	M	M	M
Palm Vein	M	H	H	M	H	M	H
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
keystroke	L	M	L	H	L	M	M

There are some success factors to be considered when implementing or purchasing a biometric system as [70]: *Accuracy:* with the great improvements of biometric systems, there is no guarantees of 100% accuracy. You are free to choose the level of accuracy you need. CER with lower percentage value is the best indicator of accuracy. *Speed:* how fast the biometric system accepts or rejects many users in a given period. *Reliability:* with system failures, the sensors must continue operating even with low CER. *Enrollment time:* is the period required for the user to finish his enrollment phase, it must be two minutes at maximum. *Data storage requirements:* is to support the biometric system used with the needed storage for user templates. User *acceptance:* the ability of the user to accept the way the system works.

3. CONCLUSION

Due to the huge raise of sensitive, personal information on cloud, the security of accessing this information becoming an important issue. This study focuses on presenting a review on various biometric and non-biometric mechanisms for accessing cloud services. As declared before, techniques like passwords, smart card tokens, etc. have a certain basic drawback in ensuring the reality of the user who is accessing which is resolved with biometric techniques of human special characteristics. From comparing physiological biometrics to behavioral biometrics, we can figure that behavioral biometrics may not be so stable and accurate due to the changes of human behaviors. But, it provides a continuous and transparent authentication to the users, which overcome the issue of static authentication in physiological biometrics authentication. Sometimes we face a drawback when using biometrics as a standalone authentication method, they could be mimicked. So, the most robust authentication techniques involve the use of more than one factor for authenticating and validating the users. Also, some physical biometrics require the use of additional hardware to support the functioning of an authentication. In our future work, we will present a model of authentication using a combination of dynamic biometric with multi other factors for providing a system with high security rate.

4. REFERENCES

[1] Mell P, Grance T, et al. The NIST definition of cloud computing. 2011;Http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Available from: http://csrc.nist.gov/-publications/nistpubs/800-145/SP800-145.pdf.

[2] Banyal RK, Jain P, Jain VK. Multi-factor authentication framework for cloud computing. In: Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on. IEEE; 2013. p. 105–110.

[3] Hogan M, Liu F, Sokol A, Tong J. Nist cloud computing standards roadmap. NIST Special Publication. 2011;35.

[4] Yang J, Chen Z. Cloud computing research and security issues. In: Computational intelligence and software engineering (CiSE), 2010 international conference on. IEEE; 2010. p. 1–3.

[5] Google. Google Apps., G Suite Gmail, Docs, Drive, Calendar and More for Business;. Accessed: 16-12-2017. http://www.google.com/apps/.

[6] Salesforce. Cloud apps and platform. CRM applications and software solutions;. Accessed: 16-12-2017. http://www.salesforce.com/eu/crm/products.jsp.

[7] Donald AC, Arockiam L. Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues. International Journal of Computer Applications. 2014;94(1).

[8] Microsoft. Microsoft Azure Cloud Computing Platform & Services;. Accessed: 16-12-2017. http://www.microsoft.com/windowsazure/.

[9] Amazon. Amazon Elastic Compute Cloud (EC2)- Amazon Web Services, Inc.;. Accessed: 16-12-2017. http://aws.amazon.com/ec2/.

[10] Amazon. Amazon Simple Storage Service (S3) â€" Cloud Storage â€" AWS;. Accessed: 16-12-2017. https://aws.amazon.com/s3/.

[11] Krutz RL, Vines RD. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing; 2010.

[12] Anzaku ET, Sohn H, Ro YM. Multi-factor authentication using fingerprints and user-specific random projection. In: Web Conference (APWEB), 2010 12th International Asia-Pacific. IEEE; 2010. p. 415–418.

[13] Modi M, Upadhaya H, Thakor M. Password less authentication using keystroke dynamics a survey. International Journal of Innovative Research in Computer and Communication Engineering, IJIRCCE. 2014;p. 7060–7064.

[14] Babaeizadeh M, Bakhtiari M, Mohammed AM. Authentication methods in cloud computing: A survey. Research Journal of Applied Sciences, Engineering and Technology. 2015;9(8):655–664.

[15] Gurav SM, Gawade LS, Rane PK, Khochare NR. Graphical password authentication: Cloud securing scheme. In: Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on. IEEE; 2014. p. 479–483.

[16] Abhishek K, Roshan S, Kumar P, Ranjan R. A comprehensive study on multifactor authentication schemes. In: Advances in Computing and Information Technology. Springer; 2013. p. 561–568.

[17] Acar T, Belenkiy M, Küpçü A. Single password authentication. Computer Networks. 2013;57(13):2597–2614.

[18] Chouhan P, Singh R. Security Attacks on Cloud Computing With Possible Solution. International Journal of Advanced Research in Computer Science and Software Engineering. 2016;6(1).

[19] Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal. 2001;40(3):614–634.

[20] Yang S, Bal G. Balancing Security and Usability of Local Security Mechanisms for Mobile Devices. Information Security and Privacy Research. 2012;p. 327–338.

[21] Ali ML, Monaco JV, Tappert CC, Qiu M. Keystroke biometric systems for user authentication. Journal of Signal Processing Systems. 2017;86(2-3):175–190.

[22] Abo-alian A, Badr NL, Tolba MF. Keystroke dynamics-based user authentication service for cloud computing. Concurrency and Computation: Practice and Experience. 2016;28(9):2567–2585.

[23] Yassin AA, Jin H, Ibrahim A, Qiang W, Zou D. A practical privacy-preserving password authentication scheme for cloud computing. In: Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International. IEEE; 2012. p. 1210–1217.

[24] Chen TH, Yeh Hl, Shih WK. An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. In: Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on. IEEE; 2011. p. 155–159.

[25] Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H. A strong user authentication framework for cloud computing. In: Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific. IEEE; 2011. p. 110–115.

[26] Nayak SK, Mohapatra S, Majhi B. An improved mutual authentication framework for cloud computing. International Journal of Computer Applications. 2012;52(5).

[27] Subramaniam T, Deepa B. Security Attack Issues and Mitigation Techniques in Cloud Computing Environments. International Journal of UbiComp. 2016;7(1):1–11.

[28] Henderson N. Hackers Use Social Engineering to Compromise CloudFlare CEO Gmail Account. http://wwwthewhircom/web-hosting-news/hackers-use-social-engineering-to-compromise-cloudflare-ceo-gmail-account. Monday, JUNE 2012;.

[29] Mondal S, Bours P. A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing. 2017;230:1–22.

[30] Matyas V, Riha Z. Toward reliable user authentication through biometrics. IEEE Security & Privacy. 2003;99(3):45–49.

[31] Meng W, Wong DS, Furnell S, Zhou J. Surveying the Development of Biometric User Authentication on Mobile Phones. IEEE Communications Surveys Tutorials. 2015 thirdquarter;17(3):1268–1293.

[32] Johansen UA. Keystroke dynamics on a device with touch screen; 2012.

[33] Wong KS, Kim MH. Towards Biometric-based Authentication for Cloud Computing. In: CLOSER; 2012. p. 501–510.

[34] Naveed G, Batool R. Biometric Authentication in Cloud Computing. Journal of Biometrics & Biostatistics. 2015;6(5):1.

[35] Vallabhu H, Satyanarayana R. Biometric authentication as a service on cloud: Novel solution. International Journal of Soft Computing and Engineering. 2012;2(4):163.

[36] Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology. 2004;14(1):4–20.

[37] Giot R, El-Abed M, Hemery B, Rosenberger C. Unconstrained keystroke dynamics authentication with shared secret. Computers & security. 2011;30(6):427–445.

[38] Monaco JV. Classification and authentication of one-dimensional behavioral biometrics. In: Biometrics (IJCB), 2014 IEEE International Joint Conference on. IEEE; 2014. p. 1–8.

[39] Olzak T. Keystroke Dynamics: Low Impact Biometric Verification. Information Security. 2006;p. 1–10.

[40] Pawle AA, Pawar VP. Face recognition system (FRS) on cloud computing for user authentication. International Journal of Soft Computing and Engineering (IJSCE). 2013;3(4).

[41] Atmakuri SM. A study of authentication techniques for mobile cloud computing. Texas A&M University-Kingsville; 2015.

[42] Padma P, Srinivasan S. A survey on biometric based authentication in cloud computing. In: Inventive Computation Technologies (ICICT), International Conference on. vol. 1. IEEE; 2016. p. 1–5.

[43] Al-Hamami AH, AL-Juneidi JY. Secure Mobile Cloud Computing Based-On Fingerprint. World of Computer Science & Information Technology Journal. 2015;5(2).

[44] Chadha A, Satam N, Wali V. Biometric Signature Processing & Recognition Using Radial Basis Function Network. arXiv preprint arXiv:13111694. 2013;.

[45] Guo JM, Hsia CH, Liu YF, Yu JC, Chu MH, Le TN. Contact-free hand geometry-based identification system. Expert Systems with Applications. 2012;39(14):11728–11736.

[46] Rassan IA, Al Shaher H. Securing mobile cloud using finger print authentication. International Journal of Network Security & Its Applications. 2013;5(6):41.

[47] Sabri HM, Ghany KKA, Hefny HA, Elkhameesy N. Biometrics template security on cloud computing. In: Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE; 2014. p. 672–676.

[48] Venakatesan N, Kumar MR. Finger print authentication for improved Cloud Security. In: Computation System and Information Technology for Sustainable Solutions (CSITSS), International Conference on. IEEE; 2016. p. 434–439.

[49] Ross A, Dass S, Jain A. A deformable model for fingerprint matching. Pattern Recognition. 2005;38(1):95–103.

[50] Aishwariya G, Kokilapriya S, Adhithya S, Selvarani AG. Fingerprint Recognition for Android Application Data Retrieval. 2017;.

[51] Deka GC. Handbook of Research on Securing Cloud-Based Databases with Biometric Applications. IGI Global; 2014.

[52] Juhola M, Zhang Y, Rasku J. Biometric verification of a subject through eye movements. Computers in biology and medicine. 2013;43(1):42–50.

[53] Abduljabbar ZA, Jin H, Hussien ZA, Yassin AA, Hussain MA, Abbdal SH, et al. Towards Efficient Authentication Scheme with Biometric Key Management in Cloud Environment. In: Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE; 2016. p. 146–151.

[54] Darve NR, Theng DP. Comparison of biometric and non-biometric security techniques in mobile cloud computing. In: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on. IEEE; 2015. p. 213–216.

[55] Delac K, Grgic M. A survey of biometric recognition methods. In: Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium. IEEE; 2004. p. 184–193.

[56] Kratz S, Aumi MTI. AirAuth: a biometric authentication system using in-air hand gestures. In: CHI'14 Extended Abstracts on Human Factors in Computing Systems. ACM; 2014. p. 499–502.

[57] Ziyad S, Kannammal A. A multifactor biometric authentication for the cloud. In: Computational Intelligence, Cyber Security and Computational Models. Springer; 2014. p. 395–403.

[58] Baloul M, Cherrier E, Rosenberger C. Challenge-based speaker recognition for mobile authentication. In: Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the. IEEE; 2012. p. 1–7.

[59] com T. Biometric Signatures;. Accessed 27-12-2017. http://www.technologyyours.com/bio-signature.aspx.

[60] Rosa L. Biometric Signature Recognition;. Accessed 27-12-2017. http://www.advancedsourcecode.com/neuralsignature.asp.

[61] Yassin AA, Jin H, Ibrahim A, Zou D. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. In: Cloud and Green Computing (CGC), 2012 Second International Conference on. IEEE; 2012. p. 282–289.

[62] Ryan S. Mobile keystroke dynamics: assessment and implementation. California State University, Northridge; 2015.

[63] Draffin B, Zhu J, Zhang J. Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction. In: International Conference on Mobile Computing, Applications, and Services. Springer; 2013. p. 184–201.

[64] Teh PS, Teoh ABJ, Yue S. A survey of keystroke dynamics biometrics. The Scientific World Journal. 2013;2013.

[65] D'Lima N, Mittal J. Password authentication using keystroke biometrics. In: Communication, Information & Computing Technology (ICCICT), 2015 International Conference on. IEEE; 2015. p. 1–6.

[66] Roth J, Liu X, Metaxas D. On continuous user authentication via typing behavior. IEEE Transactions on Image Processing. 2014;23(10):4611–4624.

[67] Miya J, Bhatt M, Gupta M, Anas M. A Two Factor Authentication System for Touchscreen Mobile Devices Using Static Keystroke Dynamics and Password. 2017;.

[68] Derawi MO, Nickel C, Bours P, Busch C. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. IEEE; 2010. p. 306–311.

[69] Jain AK, Ross AA, Nandakumar K. Introduction. In: Introduction to Biometrics. Springer; 2011. p. 1–49.

[70] Shrivasatva M. Keystroke dynamics for mobile devices–algorithm and authentication. San Diego State University. 2011;PhD diss.