

**A STUDY ON DIVERSE CLOUD INFORMATION SECURITY AND AUTHENTICATION
TECHNIQUES UTILIZING BIOMETRICS**

G. Mahesh Research Scholar, Department of Computer Science School of Computing Science,
VISTAS, PV Vaithiyalingam Rd, Velan Nagar, Krishnapuram, Pallavaram, Chennai, Tamil Nadu
600117

Dr. K. Kasturi Associate Professor Department of Computer Science School of Computing Science,
VISTAS. PV Vaithiyalingam Rd, Velan Nagar, Krishnapuram, Pallavaram, Chennai, Tamil Nadu
600117

Abstract

The examination centers around introducing a survey on various schemes of biometric authentication schemes in the cloud Background. Applying cloud computing can access information, documents, assets, application programming, working frameworks, data sets, web workers and so forth from any place whenever by means of web. The cloud computing completes more effort in not as much of time, with a smaller amount of individuals and with shared equipment and programming. Along these lines, it contributes incredible output with diminish charge. The store of organizations specialists in the cloud and stay up to date customer information across server farms which gives dangers of information spills. It is tracked down that few components have underlined on information security and in the following cycle have overlooked protection. Confirmation assists with guaranteeing and affirms a client's personality. Customary verification strategies and accreditations does not give sufficient protection after the cutting-edge methods for assaults. Thus, new biometric based verification procedures have been found to conquer the escape clauses. Biometric methods are safer as it relies on physiological and social qualities of client. So, security is significant worry in distributed computing. For validation distinctive conventional and biometrics strategies are utilized. This paper is a short outline of various biometric validation strategies utilized in distributed computing with their projected techniques and benefits.

Keywords: Cloud server, Biometric Authentication, Cloud security, Face recognition, Voice Recognition

Introduction

Cloud storage is currently an arising plan of action for information rethinking. Google Drive, Apple icloud, Dropbox, Microsoft SkyDrive and Amazon Cloud Drive. Security of re-appropriated information is basic. Encrypt the information prior to transferring to the distributed storage. As the dimension of the information is expanding, it gets hard to the customary information security algorithms utilized in cloud to encode information prior to transferring into the cloud. Customary Encryptions are bombed because of factual and word reference sorts of assaults. As a result the protection of client's information is fundamental that information can't be adjusted or seen by other than the proprietors. In this way a solid system is important to guarantee information stockpiling security. An information encryption system utilizing biometric information of an individual is proposed. It is feasible to produce a cryptographic key that is difficult to break. Client don't need to recollect or store key in their authority. There are numerous examinations on distributed computing verification methods on the subject of fine grained admittance control workers for various clients. On account of the restrictions of human memory, individuals will in general utilize same key to login to all arrange applications. Biometrics in view of their regular association with client's character and no requirement for retention, has been generally utilized.

Biometrics has by a wide margin demonstrated to be a powerful answer for a considerable lot of the security challenges that is predominant in a large portion of the specialized fields in this Digital period. The safekeeping aspect in the biometric security framework in exceptionally extemporized by connecting the information with a remarkable actual quality. The principle motivation behind biometrics in Information Technology is to serve a strategy for recognizable proof [1]. The framework is given the biometric personality such as voice test or fingerprint, which is then genuine against a put away format. It is an invulnerable safety effort which can't be crushed by

anyone which makes it a huge justification being given the principal inclination first while considering the security fundamentals regarding computer science or Cloud Computing. The two unique modes wherein biometric frameworks can be utilized are-Verification by character: This mode is utilized when the client is recently taken a crack at the framework like Identity card or login name in such a case there happens the examination between the client's biometric information and the client's information which is now present in the data set.

Statement of the Problem

To Develop a model that enhances confidentiality, Integrity and Authentication using biometrics with minimal computational time, high sensitivity and suitable for large data sets.

Objectives of the study

- To develop a model that enhance confidentiality of data stored in cloud using biometrics.
- To control unauthorized access of an user to cloud services using biometrics.
- To Preserve integrity of the stored fingerprint using hash algorithms high sensitivity.
- To develop a model that extracts minutiae from multiple types of biometrics like (Facial, Speech and fingerprint) using deep learning and
- enhance confidentiality and authentication of data stored in cloud with minimal computational time, high sensitivity and suitable for large data sets.

Review of Literature

Face confirmation or acknowledgment framework for getting versatile cloud was recommended by Deepak S and Sai Goutham N et al. They have given five phases. These are: i) Registration of User: In this stage client will download versatile application. At that point he will fill subtleties with name and letter drop ID. Letter box ID is confirmed. Entered information or data is put away in neighborhood cloud for additional utilization. ii) Face Capture: In this stage client will contact the versatile screen. At that point portable camera will be turned on. Versatile camera will catch face of client. iii) Face Detection and Face Recognition: After catching picture, in this stage face will be distinguished from the caught picture. At that point face will be perceived by removing highlights. Clients face will be coordinated with face which is put away in information base. iv) Cloud Transfer: After coordinating with face, picture will be moved to another cloud. At that point subsequent to accepting picture again it is moved to client enrolled letter drop ID. v) Screen Recording: In this stage recording begins after client actuates application. It will record screen till application is deactivated. In the wake of deactivating application recording will stop. Recorded documents will be put away in nearby memory [1].

Alaa Hussein Al-Hamami and Jalal Yousef AL-Juneidi [10] proposed multi finger biometric conspire. This plan utilizes three finger layouts of client's decision and allots single digit number for every one of these three fingers. It is utilizes during enlistment of client. Curved calculation is utilized to scramble recorded pictures and it is put away at specialist organization's end. Encryption calculation 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 finger impression acknowledgment framework with cell phone camera strategy. This strategy manages how unique mark acknowledgment is utilized to get portable could is clarified. Presently a day there is less work about utilizing computerized camera or web camera as sensor. To add separate finger impression scanner or equipment will be exorbitant. So proposed framework is utilized to get finger impression picture, through versatile camera for utilizing unique mark acknowledgment framework.

Nikhil Kumar, Dr. Yogesh Awasthi and Prof (Dr.) R.P. Agarwal [14] proposed combination of finger impression and iris biometric methods to get portable distributed computing. In this model, when client login through finger impression then twofold code is produced. This produced double code is put away in data sets of specialist co-op.

K. Marimuthu, D. Ganesh Gopal, Harshita Mehta, Aditya Rajan and P. Boominathan [21] proposed technique to settle disadvantages of One Time Password (OTP) to forestall phishing

assaults. They incorporate voice biometric procedure with one time secret word technique. This arrangement contains two interaction specifically, enlistment measure and login measure. To finish enrollment measure, client needs to give required subtleties. At that point perform CAPTCHA test to recognize people and PCs. By utilizing arbitrary capacity, novel username is created. Presently, need to supply voice secret key. When the voice secret phrase is affirmed at that point every one of client's subtleties alongside voice secret phrase is put away on the cloud. At long last, affirmation message is sent through an email.

Author(s)	Biometric method	Model / Structure	Gains
Sai Goutham N and Deepak S et al	Face	Face authentication or recognition system	This method is stress-free to appliance
Pooja Satpute and Darshan Sant et al	Fingerprint	A multiple user authentication system based on cellular controller	This technique was trivial, protected and strong. The quality of chance is high
Jalal Yousef AL-Juneidi , Al- Hamami et al	Fingerprint	Multi-finger biometric diagram	This method is modest and gives several connection options for users
HananAlShaher and IehabALRassan et al	Finger print	Fingerprint recognition method with cell phone camera	It is highly secure and also to defend booster occurrences
R. P. Agarwal and Dr. Yogesh Awasthi et al	Iris	biometric authentication techniques using Fusion	This technique is highly reliable and secure
Dr.N.Shanthi and Gokulakannan.R	Voice	One Time Password (OTP) with Voice password (VP)	It is highly protected and forceful also rises the competence
D. Ganesh Gopal, Harshita Mehta et al	Voice	voice authentication biometric practice using OpenID protocol	This procedure delivers a combined and glowing connection process

Table 1. Different biometric techniques used in cloud computing

Research Methodology

To shield the information from infection or some other obstruction from entering and extending, there are some biometric strategies which can be embraced as a safety effort in cloud computing advancements.

A. Physical Biometrics

It is one which depends on size and information separated from direct estimation of part of the body. The different driving physiological biometrics procedures are unique finger impression, retina-examine, iris-output, and facial acknowledgment and hand calculation. In Physical Biometrics, the actual impression is utilized rather than counterfeit impression for the passwords. The actual impression is immediately checked and a pathway regardless of it gets coordinated or not. If the impression gets coordinated, at that point client advances to the subsequent stage for security.

B. Behavioral Characteristics

It depends on how the individual responds to the particular conditions. Behavioral biometrics, thusly, it depend on estimations and information extricated from an activity, and they measure the qualities of the human body. Voice acknowledgment, keystroke-sweep, and signature scanner driving and significant conduct biometric advancements present in the present situation. One

of the significant qualities of a behavioral biometric is the consideration of time as an action [3]. A couple of different biometric techniques created had the option to acquire endorsement.

C. Classification of Biometric Techniques

The Identification system and Authentication system are two categories of biometric system. Contingent on attributes of biometric, consortium of various biometric strategies as demonstrated in figure 2,

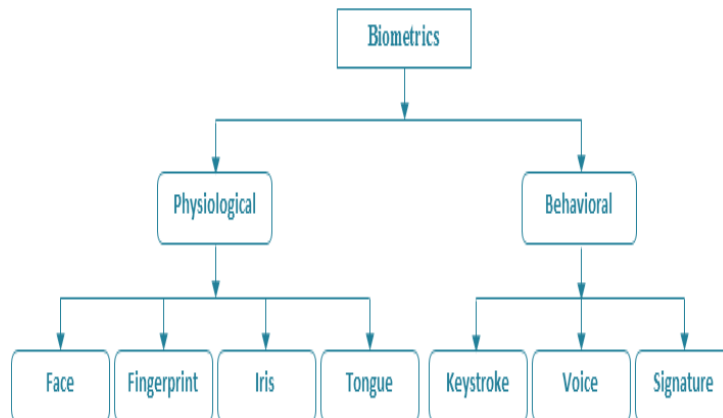


Figure 1. Biometric Techniques Taxonomy

D. Basic structure of Biometric System

The Basic structure of biometric system as shown in figure 2.

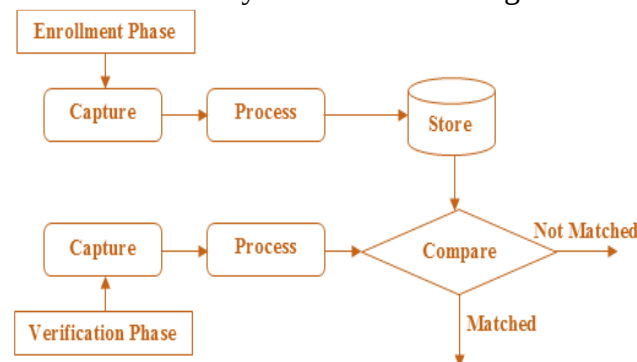


Figure 2. Rudimentary Organization of Biometric System

E. Stages of Biometric Structure

(i). **Enrollment Phase** – It consist of three stages such as capture, process and store. In capture phase, biometric mockup is caught by means of scanner or camera. In processing phase, theoretical diverse topographies from capture biometric trial via various algorithms. In store phase, mined structures from biometric trial are kept on storage tool for further acknowledgement or assessment persistence.

(ii). **Verification phase** – It likewise comprise of three phases for example capture, process and compare. This stage principally utilized for coordinating with separated highlights of caught biometric test with stored highlights. Whenever coordinated with then check is effective in any case access isn't permitted.

. Process of Authentication in Biometric sanctuary

A. Authentication Tool

Biometrics alludes to the recognizable proof of an individual character by utilizing the special physiological uniqueness. The great intention is to use the exceptional interesting actual qualities of the person for the Identity. To fill a similar need of Identity of the individual different biometric techniques have been created and are being utilized for the verification. Different kind of human qualities like fingerprints, face acknowledgment, tongue impressions and iris are the procedures utilized for biometric validation and in this way separating clients from the current

working situations. Accordingly a cloud client needs to enlist with these exceptional special qualities such as iris, fingerprints etc. While Enrollment or utilizing a help. Each time when there happens a passageway, the cloud client is animated for the provisioning of his selected characteristic or information which at that point gets contrasted and the put away layout for verification. Disregarding the uniqueness of the biometric characteristics, the issues emerge when somebody accesses the put away layouts of the attributes.

B. Working System of Biometric Security

The biometric data set of the client is kept up by the verification specialist co-op. Cryptography is utilized for putting away the information in encoded design on biometrics for security reasons. Subsequently, the client must be at first enlisted to the biometric framework given by the cloud stage or specialist organization and once after the personality enrollment the biometric validation subtleties of the individual are put away in the source information base of cloud. At the hour of enrollment, the approval subtleties or significant subtleties entered are additionally present in encoded design. Subsequently first and foremost the biometric verification administration comes right into it rather than the traditional secret word system at whatever point a client looks to utilize the cloud administrations. Whenever verification is finished, the client is then diverted to the certified cloud administration foundation of which he has been given the power.

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

Table 2. Comparative analysis of biometric techniques

Conclusion

Cloud Computing gives an assortment of administrations. In this way, it is essential to enable approved clients to access these administrations delivered in the cloud. To give cloud benefits just to the approved customer, the secure verification is essential in distributed computing. There are so many conventional confirmation procedures accessible as a secret key, One Time Password etc. Additionally there are some disadvantages as now and still secret words strategies are not feasible, the secret key can be effectively taken by programmer or if the customer uses a complex secret key, the customer may not remember. From this secret word and etc so that it is a superior choice to use biometric verification procedures as opposed to conventional confirmation methods. In summary, as biometrics plan to enhance security, the hosting we can say that the combined biometric validation frame can be expressed as a new response to verify clients on distributed computing that can be administered as administration on the Cloud and can be worn or swearing as a solitary sign on. This Study deals with different biometric verification procedures such as various creators for the distributed computer climate. We inspect extravagant all these strategies. From this study, we deduce that biometric validation procedures give new answers to check the client in distributed computing. In addition, it offers a decent establishment for an additional review to provide security in distributed computing.

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](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. P. Padma, S. Srinivasan. "A survey on biometric based authentication in cloud computing", 2016 International Conference on Inventive Computation Technologies (ICICT), 2016
5. 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.
6. Google. Google Apps., G Suite Gmail, Docs, Drive, Calendar and More for Business;. Accessed: 16-12-2017.
7. <http://www.google.com/apps/>.Salesforce. Cloud apps and platform. CRM applications and software solutions;. Accessed: 16-12-2017. <http://www.salesforce.com/eu/crm/products.jsp>.
8. Donald AC, Arockiam L. Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues. International Journal of Computer Applications. 2014; 94(1).
9. Krutz RL, Vines RD. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing; 2010.
10. 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.
11. 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.
12. Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security", 2014 International Conference on Computer Communication and Informatics, 2014.
13. 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.
14. 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.
15. 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.
16. Acar T, Belenkiy M, Küpçü A. Single password authentication. Computer Networks. 2013;57(13):2597–2614.
17. 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).
18. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal. 2001;40(3):614–634.
19. Yang S, Bal G. Balancing Security and Usability of Local Security Mechanisms for Mobile Devices. Information Security and Privacy Research. 2012;p. 327–338.
20. 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.
21. 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.
22. 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.