International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Biometric Authentication for the Cloud Computing

Tejas Sunil Kale

MCA,MET Institute of Computer Science, Mumbai

Dr. Harshali Patil

Associate Professor

MET Institute of Computer Science, Mumbai

Abstract: -

Currently cloud computing is becoming a popular trend in IT industries. Many of the Enterprises / Businesses are using cloud for storing and maintaining their huge data on cloud servers. Early security was given by password and pin codes, by this hackerare able to crack these passwords easily so data is not secure until we have a secure mechanism to protect data/confidential information fromthe hackers. So, it is more important to make sure that the security of confidential business data in cloud storage along with making sure that only authorized person can access the application or data in the cloud. So here comes biometric security in the picture it increases competencelevel of security and allowing only authenticated individuals by verifying their biometric parameters. It includes patterns like fingerprints, face, voice, retina, iris, DNA recognition etc. Implementing this biometric system into cloud will make security of data to higher level. This paper come up with to enhance the protection of creating the biometric key from the fingerprint biometric with feature extraction. Therefore, it is unique and provides fast and contact-less authentication

Introduction: -

Cloud computing is considered a new point of view of service-based utility computing where a business industry needs to reimburse only for the services needed, apart from putting work in setting up the entire infrastructure or gathering license for a whole business software. Sobasically, cloud computing has turned the way of people perception about services and computing. it has the provision of allocating the storage resources, network resources to multiple clients at a single time on daily basis. It elevated the customers from the problem of purchasing and maintaining the entire IT infrastructure and let them focus primarily on their business issues.

Cloud computing brings down the cost of any business organization by providing scalable, configuring devices. It provides services based on storage,software, and platform. There are basically three models Platform as a Service,Infrastructure as a Service and Software as a Service and Deployment models are Public Cloud, Hybrid cloud, Private cloud Community Cloud. The figure 1.0shows the cloud computing model

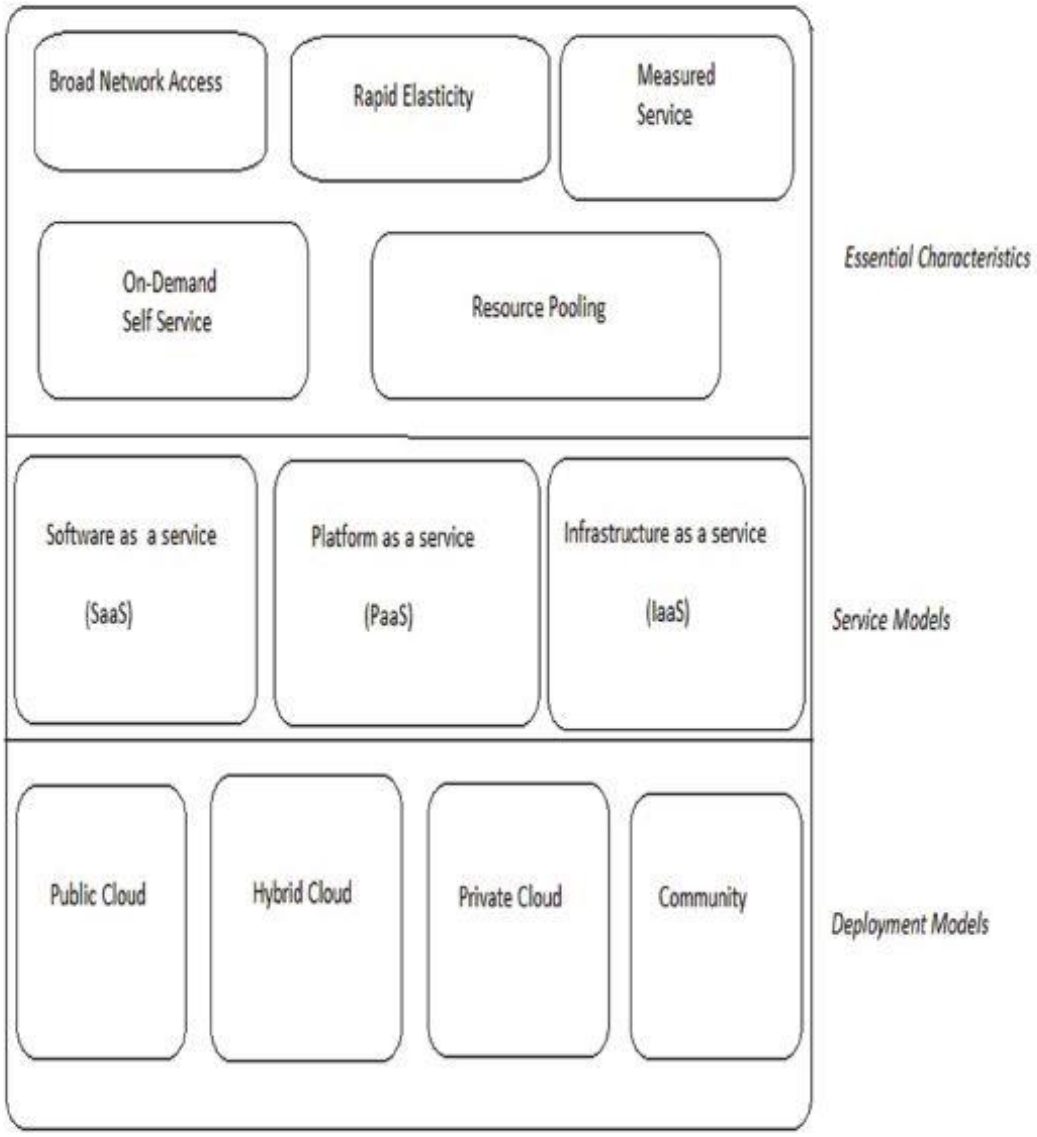

Figure 1.0 Cloud Computing Model

Need for Security in cloud computing: -

The main issue is not about the security mechanism that is being applied on the data or stored in remote location, but it is about "How much the particular environment is safe?" Risks are defined on basis the nature of threats and possibility of attacks the major issue are about Data Confidentiality, Data Integrity, and Data Availability

System Architecture: -

We can use different techniques for providing security to cloud. Usually, passwords are used for authentication, but the thing is passwords are easily attackable. Instead, we can use biometric authentication techniques which can used for securing cloud computing as displayed in the Figure 2.0

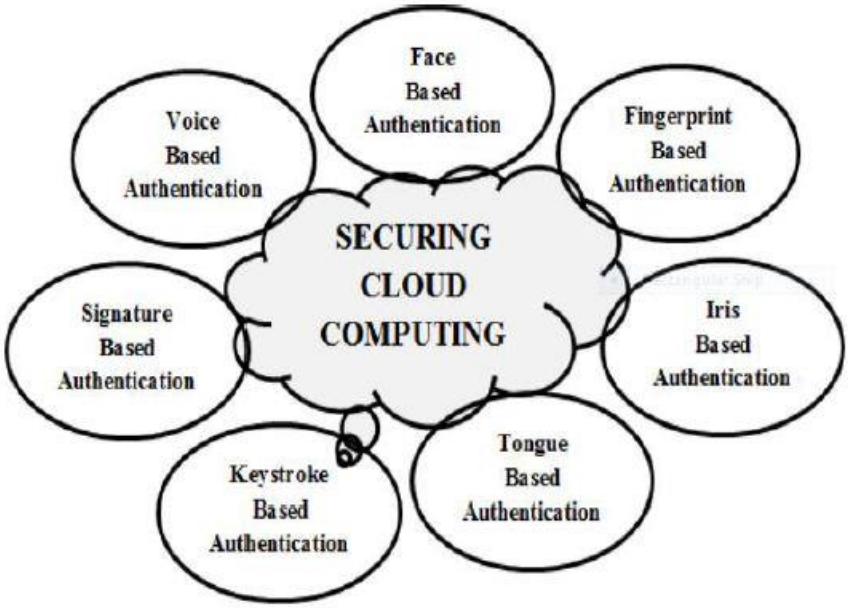

Figure 2.0 Biometrics technique to secure cloud computing

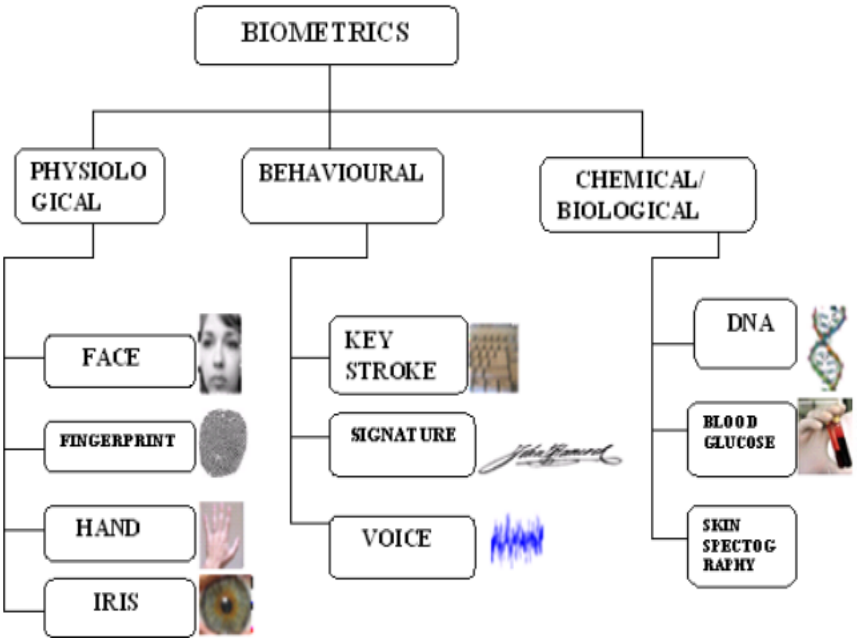

Figure 3.0Biometric characteristics: Physiological characteristics and behavioural characteristics

Figure 3.0 states that classification of different biometrics based on physiological, behavioural, and chemical/biological. We would be more focusing on physiological and behavioural characteristics.

Enhancement of security

Cloud based services are usually accessed through a web-based user interface that can either be a mobile application or web browser. The cloud service provider manages cloud-based biometrics and is available on demand. It includes a server that contains the biometric templates databases along with the processing data generated during the identification and verification for cloud users. Certain problems might arise if untrustworthy individuals obtain access to the databases of biometric templates, even if the biometric traits are unique, so by utilizing encryption technology biometric authentication takes care of these types of security threats.

Here, Encryption states that the method of converting data into a pattern that cannot be understood by unauthorized individuals and decryption states that transforming data back to its original form so that it could be understood.

Suppose a hacker is able toobtain access to a fingerprint image he won't be able to decrypt it to the original image because, the fingerprint images are encrypted at the both the user's along with the service provider's end by using encryption algorithm for providing better security.

Mode of operations of biometric system

Biometric system may function either in the identification or verification mode based on the application context. In identification mode the input user image is matched against a set of labeled user images in a database. In negative recognition application identification is a critical component, the main scope of this is to hinder a single person from utilizing multiple identities. Here biometric system is demonstrated as a Pattern Recognition Systems where input user's image is compared against the feature sets of other images to determine their identity.

Where verification mode is a method for positive recognition where the main motive is to avoid multiple subjects from using the similar/same identity of individuals.

Following table 1.0 shows analysis of biometric techniques based on different parameters. After the analysis of different biometric techniques based on the different parameters we can state that fingerprint has more consistency overall as compared to face, iris, voice and signature.

Parameters / Biometric Techniques	Fingerprint	Face	Iris	Voice	Signature
Device	Scanner	Camera	Camera	Microphone	Touch Panel, Optic pen
Cost	Medium	Medium	High	Medium	Medium
Accuracy	High	Medium low	High	Medium	Low
Interference	Injury, Dirtiness	Glasses	Glasses	Noise, Cough, Cold	Easy Signature
Reliability	High	High	Very High	High	High
Acceptance	High	High	Medium Low	High	High
Stability	High	Medium	High	Medium Low	Medium Low
Identification and Authentication	Both	Both	Both	Authentication	Both

Table 1.0 Analysis of biometric techniques based on different parameters.

Literature Review: -

In this survey, we reviewed the works published in recent three years by searching articles from different journals. The keywords we used in the search comprises of biometric authentication, iris, face, fingerprint, recognition and so on.

[5] Al-Assam, Hassan &Zeadally (2019) surveyed about authentication method based on biometrics in cloud environments. Talking about cloud data, authentication based on traditional method lacks security/Safety. This concludes, multifactor authentication is suggested which permits two or more authentication parameters alongside with password-based security this review focuses on the advantages and disadvantages of different available biometric authentication models.

[6] Dulari and Bhushan (2019) suggested an authentication method for various user in distributed environment based on cloud computing. They proposed system for cloud storage called TORDES to avoid unauthorized access the data is stacked in TORDES for authentication with crypto-biometric systems.

[7] Shabbir et al. (2021) mentioned noticed profits of Mobile Cloud Computing in medical healthcare. Using Modular Encryption Standard (MES) they implemented layered security modelling to increase the safety of MCC. It addresses difficulties in privacy and security of customer data. The performance was good than the other encryption techniques.

[8] Yellamma, Pachipala, P. S. Rajesh (2020) proposed efficient and privacy conserving biometric identification theme in cloud computing. They designed a brand-new coding rule and cloud authentication, to improve security and efficiency needs and will resist the potential attacks.

[9] Barni, Mauro and Giulia Droandi (2019) proposed a multimodal authentication protocol names SEMBA based on SPDZ tool, this is to secure against a malicious party. They suggested without loosing any accuracy, evaluation time it is possible to improve the efficiency of recognition process using a multi-modal system. Here they adapted the iris and face authentication protocols in SPDZ tool this could also reduce the further additional complexity.

Model Applications :-

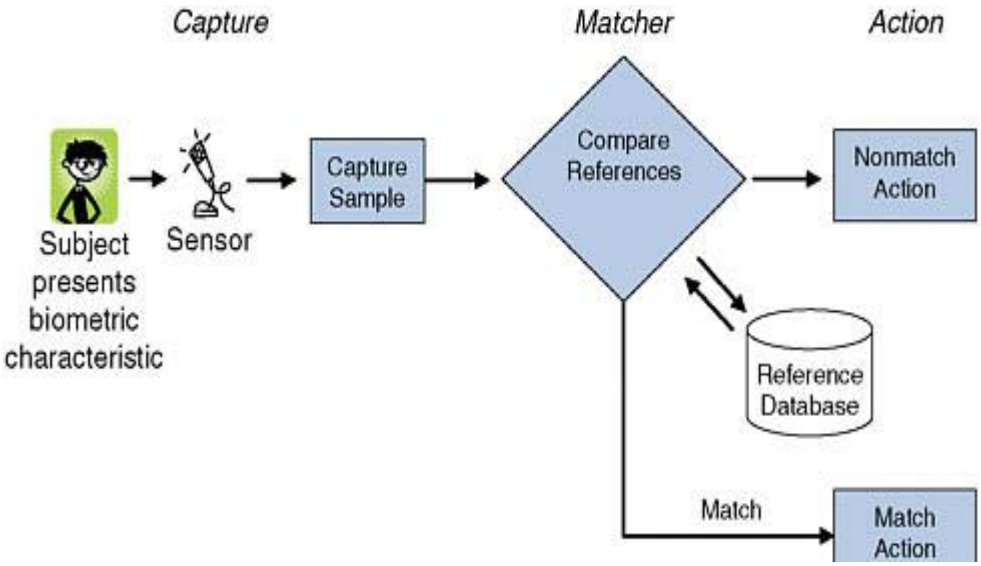

Figure 4.0 System model of biometric system

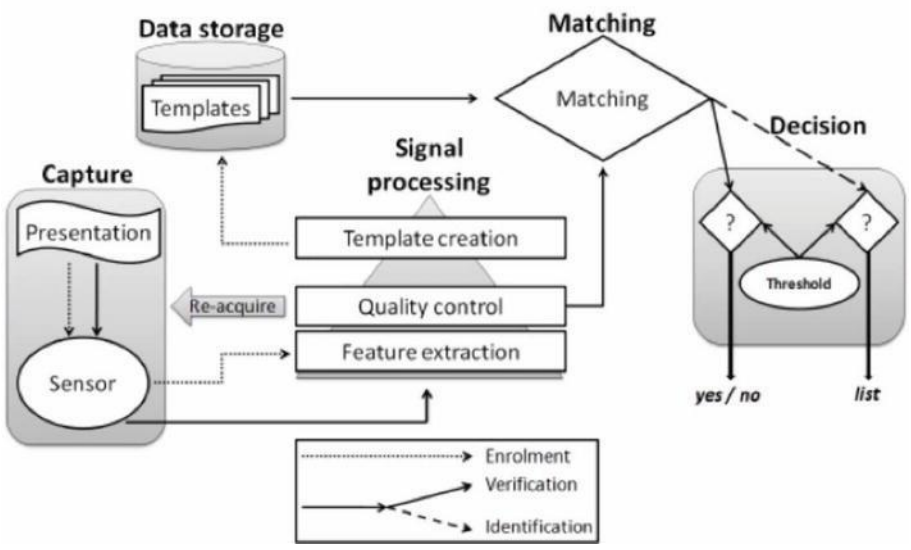

Figure 5.0 Activity diagram of biometric application

The above diagrams shows the flow of biometric system in terms of data storage and process.

Proposed system: -

Srno.	Type of Biometric Technique	Proposed Method/ Technique	Advantage(s)
1	Fingerprint	A multiuser authentication scheme supported on cellular automata	Lightweight, Secure, and robust
2	Face	Face authentication or recognition system for securing mobile cloud	Easy to use and implement.
3	Iris	Cloud Iris Verification System (CIVS)	Relatively simple and secure
4	Voice	Voice password with One Time Password (OTP)	Highly secure and robust

Table 2.0 Summary of different Biometric Techniques

The table 2.0 explains the summary of different biometric techniques and their proposed method and advantages. We proposed total of four different biometric techniques. For new user whenever he/she wants to approach the cloud the first thing he/she should do is to list by their fingerprints. After registering he/she turned into a valid user and couldlog on to the cloud. By using Advanced Encryption Standard Algorithm fingerprint images is stored and then encrypted. It will then provide a secret key to the user and used for high security purpose.

After the process of Advance Encryption Standard Algorithm is done, then feature extraction is performed on encrypted data. So basically, it takes the mean of all the blocks from Advanced Encryption Standard algorithm. This mean is then compared with the means of data that is already stored in the database while the user registers it. Advanced Minutiae Base Algorithm is used for process of matching. It compares the two images and gives the result if whether a user is valid or not.

Results:-

The findings/ research we proposed through this paper is different types of biometric techniques and its features and advantages over one another. As mentioned in table 1.0 Analysis of biometric techniques based on different parameters after analyzing and study we found that fingerprint and iris are some of the best approach in biometric environment. Along with this we also reviewed different research paper suggesting

different techniques of biometric system and found multiple tools and authentication approach used, and after the process of scanning/ gathering data through biometric mean we suggested advanced encryption standard and advanced minutiae base algorithms to utilize.

Discussion: -

As we know that by using biometric system there are also some limitation that we would face. One of the limitation is cost, many sensors are of high cost like fingerprint sensor, web cam etc. To tackle this is we can use refurbished or recycled products. Future work for this would be introducing new algorithms which might useful in terms of processing speed, cost effective, efficient, etc.

Conclusion: -

This paper proposes biometric authentication for cloud computing. Cloud service providers provides the service to users on pay only for use strategy. For these types of services, safety is a major concern. To overcome the security issues biometric authentication is used along with two proposed algorithms Advanced Encryption Standard Algorithm and Advanced Minutiae Base Algorithm. Various kinds of sensors are used, biometric authentication technique too have some drawbacks. We also stated the analysis of biometric techniques and their efficiency based on different parameters. To tackle this issue, we can use multi-model authentication scheme using more than one biometric technique. In the future, for checking data duplication Standardized intelligence algorithm could be further used and for user authentication different biometric techniques can be expanded.

References: -

[1] AES trends 2022: - https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[2]Lu, Yanrong, and Dawei Zhao. "Providing impersonation resistance for biometric-based authentication scheme in mobile cloud computing service." Computer Communications 182 (2022): 22-30.

[3] R. Kannavara, N. Bourbakis, N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou, "A comparative survey on biometric identity authentication techniques based on neural networks" in Biometrics: Theory Methods and Applications, pp. 47-79, 2009.

[4] A. K. Jain, A. Ross, and S. Prabhakar, An introduction to biometric recognition, IEEE Trans Circuits Syst. Video Technology, Special Issue Image and Video-Based Biomet, Volume 14, Issue 1, Jan 2004, pp. 4–20.

[5] Al-Assam, Hisham, Waleed Hassan, and SheraliZeadally. "Automated biometric authentication with cloud computing." Biometric-based physical and cybersecurity systems. Springer, Cham, 2019. 455-475.

[6] Dulari, Pawitar, and Brijender Bhushan. "A novel approach for cloud data security enhancement through cryptography and biometric in the government cloud environment." International Journal of Computer Science and Mobile Computing 8, no. 12 (2019): 59-63.

[7] Shabbir, Maryam, Ayesha Shabbir, Celestine Iwendi, Abdul Rehman Javed, Muhammad Rizwan, Norbert Herencsar, and Jerry Chun-Wei Lin. "Enhancing security of health information using modular encryption standard in mobile cloud computing." IEEE Access 9 (2021): 8820-8834.

[8] Yellamma, Pachipala, P. S. Rajesh, V. V. Pradeep, and Y. B. Manishankar. "Privacy preserving biometric authentication and identification in cloud computing." Int. J. Adv. Sci. Technol 29 (2020): 3087-3096.

[9] Barni, Mauro, Giulia Droandi, Riccardo Lazzeretti, and Tommaso Pignata. "SEMBA: secure multi-biometric authentication." IET Biometrics 8, no. 6 (2019): 411-421.

[10] Golec, Muhammed, Sukhpal Singh Gill, Rami Bahsoon, and Omer Rana. "BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0." IEEE Consumer Electronics Magazine (2020).