Applied Science & Engineering Journal for Advanced Research
ISSN (Online): 2583-2468
Volume-1 Issue-4 || July 2022 || PP. 28-33 DOI: 10.54741/asejar.1.4.6

An Approach to Biometric Encryption in Cloud Computing

Kiran Jain
Associate Professor, School of Computer Applications, Babu Banarasi Das University, Lucknow, Uttar Pradesh, India

Corresponding Author: kiranc1975@gmail.com

Received: 12-06-2022 Revised: 30-06-2022 Accepted: 14-07-2022

ABSTRACT
Security concern has become the biggest obstacle to adoption of cloud because all information and data are completely under the control of cloud service providers. Cloud data encryption is not the solution for data whichcan keep faith over cloud security.Biometric encryption has been provided for cloudconsumer's valuable information and identity verification has been utilized in a unique way.Biometric encryption is proposed to improve the confidentiality in Cloud computing for biometric data. When it comes to biometric data, such as face reorganization statistics for prominent and significant persons, the confidentiality of a specific user is a concern. In this study, a hybrid authentication approach that is dependent on biometrics and encrypting technologies is created for the security of cloud-based computation.The above study uses sophisticated encryption standards as a reliable encryption method and fingerprints as a biometric technology to create secure and robust technology. This brings us to the crucial parts on biometric technologies for cloud computing, where we describe cutting-edge strategies that provide quick and private authenticating required for cloud environments.

Keywords: *biometric encryption, cloud computing, privacy, security, authentication, fingerprint, blowfish algorithm, cloud service access, identification*

I. INTRODUCTION

Organizations frequently adopt cloud computing to store vast amounts of data in the clouds. When using cloud computing approaches, you can get a wide range of services, such as "platform-as-a-service, infrastructure-as-a-service, and software-as-a-service, where its simulation securities really represent the service strategy". A technique known as cloud computing allows users to raise or decrease their storage space on demand while having to construct new infrastructures. Current developments in technologies like virtualization technology; Web applications, distributed systems, ubiquitous computing, and main application have given rise to cloud computing. Data protection is achieved through encryption, and accessibility to protection of personal data is made possible by key generation. We shall discuss data security in the cloud when describing data encryption and decryption.

Whenever transferring cloud information from specific storage to the cloud, cloud security offers data encryption services that encrypt the data so that it is difficult for any application or database to decrypt it [1].An inventive concept for cloud based identification utilizing encrypted biometric security has suggested many techniques to preserve biometric information employing various encryption techniques[2].To ensure safe communications, cloud systems must be enabled with advanced security features such homomorphic encryption cryptography, differentiated privacy rights technologies, backup and recovery components, etc. [3].

For further protect applications and information stored in the cloud, key distribution and encryption are both crucial[4].The authentication process must first gather biometric information from several individuals before establishing a secure connection[5].Therefore, it appears that security issues are being reduced by biometric authentication that is based both on physical and behavioral cues[6].Biometric security methods detect and recognize face, finger prints, iris, retina, ear shapes, and more[7].

Biometrics solutions are drawn to the cloud's promise qualities. Information can be moved from biometric verification to cloud backups or computation. Including its powerful authentication capabilities, biometrics may be used by the clouds to improve security and provide new service paradigms [8].

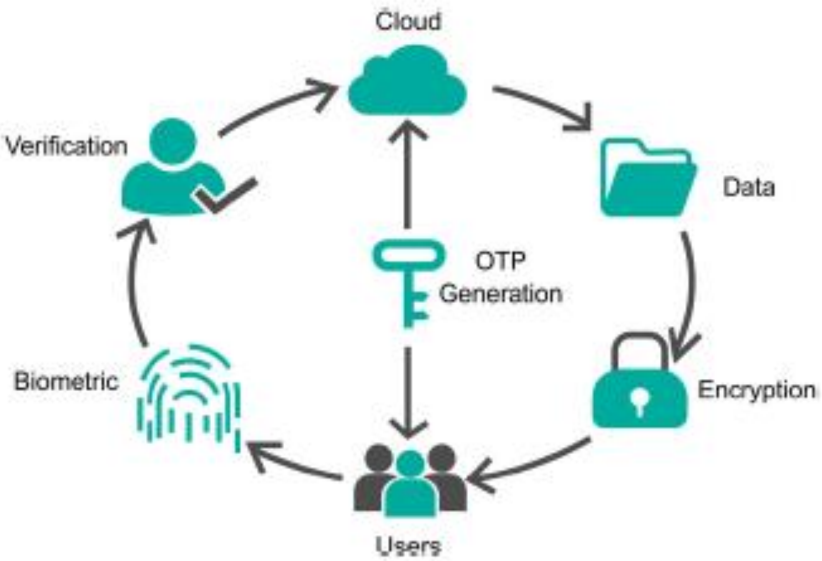

Figure 1: Proposed hybrid model

II. LITERATURE REVIEW

Here on base of author’s research, this portion of the literature review discusses various crucial biometric identification mechanisms, techniques, and statistics.

R. Arun Prakash et.al 2018 explained byto solve all the security issues in cloud environments, "BEBA (Biometric encoding and Biometric authentication)". An inventive concept for cloud security identification utilizing encrypted biometric security has suggested many techniques to secure biometric information using various encryption methods. Various cryptographic mechanisms have been employed to secure both the verification system and data stored in the cloud, but these techniques must be applied in the right places and sensitive spots. Due to the vast amount of data in the cloud, blowfish encryption has been deployed. When compared to other encryption techniques, the computation performance of blowfish is indeed very significant[2].

Dr. D.B.K. Kamesh et.al 2017 described by Because they are based on a customer's physiological and behavioural features, biometric approaches are more secured. Three fundamental ideas “Service models (SaaS, PaaS, and IaaS), deployment patterns (public, private, community, and hybrid), and many key attributes are the foundation of cloud computing architectures”. The two fundamental tenets of cloud computing are distributing and pay-per-use. In cloud computing, secured authentication is essential to only offer cloud storage to authenticate users[9].

Mehreen Ansar et.al 2018 explained by The most reliable way of authentication is biometric. The scientific word for estimating and quantifying various bodily elements by connecting measures to human attributes is biometrics. Realistic identity is controlled by biometric authentication, which is specific to each person or group. When creating a secret key for security, “the Advanced Encryption Standards algorithm extracts features from fingerprints biometric using a technique referred to as the Advanced Minutiae Base Algorithm (AMBA)”. A feature selection method, sensor, and matching components or subsystems are combined in biometrics to apply detection algorithm on a specific biometrics characteristic [10].

Manisha et.al 2017 described by Data is encrypted using the blowfish algorithm so that it cannot be readily deciphered, and authenticity is accomplished through biometric fingerprints. A cryptography accessing control scheme is used for information protection and integrity, and biometric features with fingerprints are used to offer authentication safety. The term "biometrics" describes the use of distinctive physiological traits to determine a person's identity. It must be encrypted immediately before being stored or uploaded to the cloud. The process of transforming data into a format that is difficult for unauthorised individuals to understand is known as encryption [11].

Zarnab Khalid et.al 2019 described by in cloud computing, data protection is becoming increasingly essential. A biometric is a physical feature that can be used to recognize individual using computers. A real benefit for the cloud service is biometric. Due to the admissibly unique characteristics of biometric features, bio-cryptography was used to protect the cloud server utilising key bindings to establish a cryptographic key. Biometric technology is mostly employed in both security and networking systems. In computer programming, biometrics is used for authentication and security systems. Biometric authentication uses quantifiable traits to determine individuality [12].

Mr.Satish Manje et.al 2020 introduced by consequently, the biometric information is transferred to a cloud platform and is encrypted. But, while transferring this biometric information to the cloud, it must be secured in order to protect and guarantee its confidentiality. The request information is encrypted by the data holder before being sent to the cloud to implement a biometric authentication system. A dependable and trustworthy method for recognizing people is biometric identity. Strong encryption security and protection towards potential hacking attempts, loss of data, and misuse are essential for the widespread implementation of this biometric identity [13].

Md. Alamgir Hossain et.al 2022 evaluated by Biometrics is the utilization of a person's unique physiologic, sociological, and architectural hallmark to supply productive individualized ID. Homomorphic encryption is used in the encryption method, and the clients region is used in the decoding stage. In order to enhance security and prevent data from being accessed from the clouds by unauthorized parties, we presented a hybrid verification system that relies on biometrics and encrypting frameworks. For authentic client validating, a hybrid confirming framework based on biometric and encryption performs better than a standalone biometrics checks and encrypted architecture. Just using encryption or anonymity to store data in the cloud is insufficient [14].

B Naga Raju et.al 2021 defines by A more advanced version of the data preparation administrative authority available in the educational now can be found in cloud computing. Techniques for validating biometrics are broadly divided into two categories, namely physiological biometrics and socially biometric traits. Biometric technology refers to the identifying evidence of a person based on their biological features or behavioral traits. The person will be verified at the start of the actual engagement with a biometric identification mechanism. The DNA-based biometric framework is intrusive yet not easily updated. Biometric data is examined for accuracy [15].

Sarita Motghare et.al 2021 proposed by The biggest obstacle here is coming up with a technique for an effective and trustworthy biometric authentication system to safeguard cloud security. The expansion of cloud computing has prompted personal information to spread the vast amount of biometric information. Usage of biometrics, namely to carry out a biometric authentication,the majority of biometric security processes should be carried out in the cloud to improve efficiency. The fundamental concept behind cloud computing is virtualization. The widely used cloud storage administration method known as "cloud computing" allows the data owner to keep sensitive data across several clouds[16].

Kulsum Subiya et.al 2022described by as a component of this project, novel biometric identification techniques are being developed for better accessibility to remote (cloud) servers. The user's biometric information is then applied to generate a distinct character for them, safeguarding their privacy in the process. It successfully safeguards the safety of particularly sensitive cloud-based information and documents while also efficiently preserving the privacy of cloud services. Biometric recognition technologies are therefore better suited for preserving the biometric details of cloud applications. The protection of sensitive data (such as biometric information as well as other data) and the protection of personal details are crucial considerations when it comes to authentication process in cloud computing.Therefore, the security and confidentiality of specific users can be guaranteed through the incorporation of biometrics encrypting data in biometric authentication technologies[17].

III. METHODOLOGY

Showing how to select, verify, and save templates for basic identification in cloud technology. This research article's main goal is to securely save and recover fingerprint template from cloud servers. Accurate identity is controlled by biometric security, which is unique to each individual [10].

Users can employ a variety of approaches to secure the clouds. Username and password are typically used for verification. However, passwords can be quickly cracked. That technique is the easiest and most affordable. Therefore, we can employ biometric verification to give cloud computing security. As seen in fig. 2, biometric identification methods are employed to secure cloud computing.

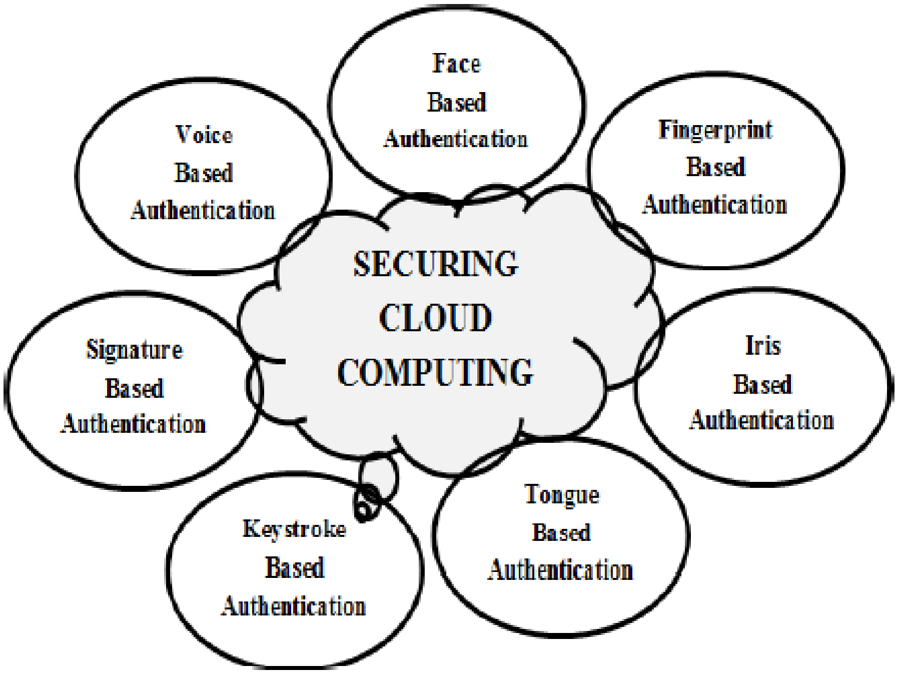
Face Based Authentication
Voice Based Authentication
Fingerprint Based Authentication
SECURING CLOUD COMPUTING
Signature Based Authentication
Iris Based Authentication
Keystroke Based Authentication
Tongue Based Authentication

Figure 2: Biometric Technologies for Cloud Computing Security [9]

The user-provided biometric information is encrypted using the "Advanced Encryption Standard (AES) encryption technology"[18].The encrypted information is subjected to identification procedures by the cloud, which then provides the owners of the database with the results. But just before exporting, the biometric data must be encrypted in order to protect its confidentiality. Identity-based encrypting and biometrics are a part of the safety data access system for the cloud. The e-voting method is made better secured and authenticating by biometric identification. Additional encryption techniques will be developed in future projects[19][20]."The Key Policy Attribute based Encryption approaches, which include several image analysis and encrypted methods, are used in the biometric encryption method" [21].

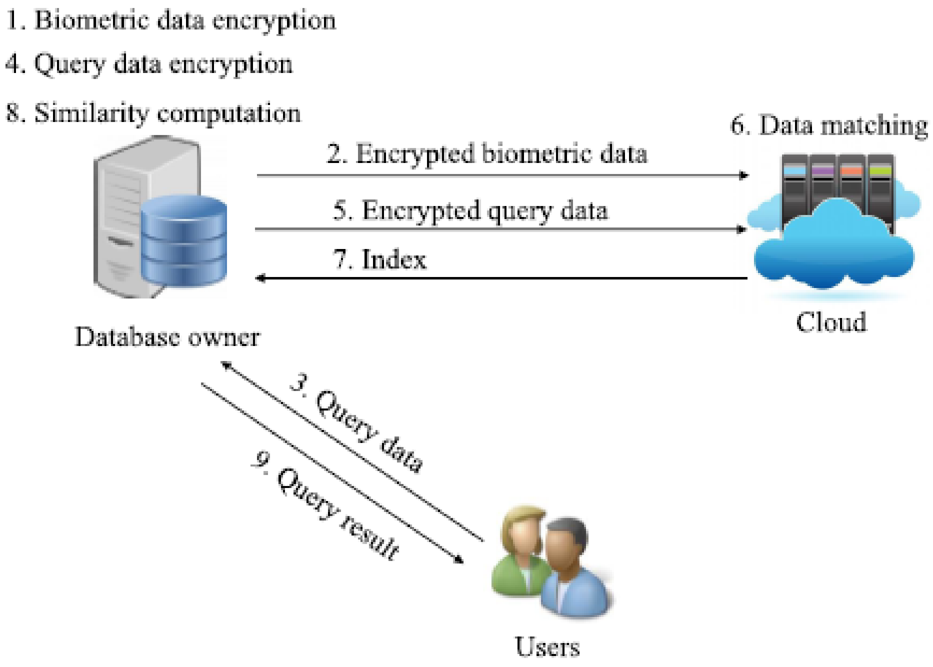

Figure 3: Model proposed for biometrics encryption

The databases owners, viewers, as well as the cloud are three different sorts of objects that are associated with the system, as depicted in Fig. 3. Every owner of the databases is in possession of a sizable amount of biometric information, such as fingerprinting, iris recognition, speech styles, and facial shapes, which is sent and stored in the cloud using encryption. A search response is issued to the contains records whenever a user chooses to be recognized. Following the receipt of the request, the information owner creates a ciphertext for the requested biometric characteristic and sends it to the clouds for authentication.The cloud server selects the most usually considered for the encryption request and gives the information administrator the relevant indexes. In order to retrieve the user's request message, the databases owners evaluates the similarities between both the identify and analyze and the biometric information connected with the indexes [22].

As a practical method to recognize people, biometric-based authentication, which depends on individual's physiological or behavioural features, is becoming more and more popular. “The term biometrics relates to an authentication method that instantly measures distinctive physical features like the fingerprint, voice, ear, eye color, iris, and palm print”. The major advantages of biometrics are “(1) higher level of security of stored data (2) privacy preservation of users (3) diminutive chances of forgery and (4) cost-effective based solutions and (5) user friendliness”. Since, encryption is the conversion of data into a form that cannot be easily understood by unauthorized people [23].

Employing biometrics encrypting for biometric information also improves privacy in cloud computing. The cutting-edge method of biometric encryption aims to improve the privacy of biometrics data in cloud computing. A method for securing biometric identification is called biometric encryption (BE). Recent times, the economic viability of dispatching biometric encrypted communications have been performed for mobile Cloud services. Consequently, it is strongly advised that biometric encrypted data be used in cloud computing [24].

IV. CONCLUSION

In order to avoid the significant costs of processing and storage, databases administrators are tempted to outsourcing identification activities and significant amounts of biometric information to the cloud. This, although, raises possible privacy risks for consumers. The paradigm of cloud computing, which is constantly changing and acquiring new characteristics and capabilities, is used to preserve most of the information. In cloud computing, reliable authentication is essential to only offer cloud storage to authenticate users. Utilizing a biometric identification solution significantly raises the secure communication of a cloud service in aspects of identity verification.Among the most cutting-edge and secured methods for biometric authentication in cloud computing is this method. Every process involving the biometric characteristics has different advantages and disadvantages. Since we employed finger print technology along with other encryption techniques and a larger amount of cloud storage, a same task can be done in the future using various biometrics.

REFERENCES

[1] J. Kumar. (2019). Cloud computing security issues and its challenges: A comprehensive research. *Int. J. Recent Technol. Eng.*, *8*(1), 10–14.

[2] R. ArunPrakash, T. Jayasankar, & K. Vinothkumar. (2018). Biometric encoding and biometric authentication (beba) protocol for secure cloud in M-commerce environment. *Appl. Math. Inf. Sci.*, *12*(1), 255–263. doi: 10.18576/amis/120126.

[3] M. N. Sharath, T. M. Rajesh, & M. Patil. (2019). Analysis of secure multimedia communication in cloud computing. *2019 2nd Int. Conf. Intell. Comput. Instrum. Control Technol.* pp. 136–144. doi: 10.1109/ICICICT46008.2019.8993352.

[4] S. Nandan Kumar, & A. Vajpayee. (2016). A survey on secure cloud: security and privacy in cloud computing. *Am. J. Syst. Softw.*, *4*(1), 14–26. doi: 10.12691/ajss-4-1-2.

[5] T. N. Nguyen, & T. T. T. Le. (2022). Authentication and encryption algorithms for data security in cloud computing: A comprehensive review. *Proc. Sixth Int. Conf. Res. Intell. Comput.*, *27*, pp. 57–63. doi: 10.15439/2021r7.

[6] J. V. Rosy. (2021). Biometric security for cloud data using fingerprint and palm print. *Sample Fingerprint*, *IX*(Ii), 58–67.

[7] P. Tiwari, & A. Saklani. (2013). Role of biometric cryptography in cloud computing. *Int. J. Comput. Appl.*, 70(9), 34–38. doi: 10.5120/11993-7874.

[8] S. Gawade, A. Bharti, A. Raj, & S. Madane. (2017). Biometric authentication using software as a service in cloud computing. *Int. J. Eng. Comput. Sci.*, *6*(3), 20410–20413. doi: 10.18535/ijecs/v6i3.01.

[9] Akshay A. Pawle, & Vrushsen P. Pawar. (2017). A study of different biometric authentication techniques in cloud computing. *Int. J. Eng. Res.*, *V6*(05), 612–619. doi: 10.17577/ijertv6is050575.

[10] M. Ansar, S. Arshad, N. Nazir, & M. Fatima. (2018). Biometric encryption in cloud computing: A systematic review. *Int. J. Comput. Sci. Netw.*, *6*(1), 10–19.

[11] S. Rani. (2013). *Hybrid security approach for cloud using fingerprint and blow fish algorithm*.

[12] Z. Khalid, M. Rizwan, A. Shabbir, M. Shabbir, F. Ahmad, & J. Manzoor. (2019). Cloud server security using Bio-

cryptography. *Int. J. Adv. Comput. Sci. Appl.*, *10*(3), 166–172. doi: 10.14569/IJACSA.2019.0100321.
[13] S. Issue. (2020). *An efficient biometric identification system*.
[14] M. A. Hossain, & M. A. Al Hasan. (2022). Improving cloud data security through hybrid verification technique based on biometrics and encryption system. *Int. J. Comput. Appl.*, *44*(5), 455–464. doi: 10.1080/1206212X.2020.1809177.
[15] B. N. Raju, A. M. Rao, S. V. Siva, N. Raju, & V. Sevanth. (2021). *Integrating biometric mechanism to protect user data in cloud computing*.
[16] S. M. Et. al. (2021). Implementation of privacy preserving and dynamic searching mechanism with biometric authentication in cloud storage. *Inf. Technol. Ind.*, *9*(2), 894–912. doi: 10.17762/itii.v9i2.427.
[17] M. T. (2022). *Enhanced security schemes in cloud*.
[18] M. Nikam, P. Dupargude, P. Patil, D. Jadhav, & R. Dongare. (2018). Secure file access using biometric security and key share among cloud. IJIRSET , 6326–6329. doi: 10.15680/IJIRSET.2018.0705228.
[19] V. Naresh, T. Gopi Venkata Ajay, T. Naga Sai Reddy, & M. Srinivas. (2020). An efficient and privacy preserving biometric authentication scheme in cloud computing. *Int. J. Sci. Technol. Res.*, *9*(1), 1966–1969.
[20] Chakraborti Bratati. (2015). E-voting security system through biometric cloud computing integration with virtual server application. *Eur. J. Acad. Essays*, *2*(1), 6–9. Available: www.euroessays.org.
[21] S. Rinesh, & M. Mohanapriya. (2015). *Secure and efficient data sharing in cloud using hybrid patient controlled biometric encryption scheme*.
[22] L. Zhu, C. Zhang, C. Xu, X. Liu, & C. Huang. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access*, *6*, 19025–19033. doi: 10.1109/ACCESS.2018.2819166.
[23] D. Raja, T. Bhalodia, & R. Buch. (2020). *Review on biometric two-way authentication in cloud computing*.
[24] M. N. Omar, M. Salleh, & M. Bakhtiari. (2014). Biometric encryption to enhance confidentiality in Cloud computing. in *Proc. - 2014 Int. Symp. Biometrics Secur. Technol.*, pp. 45–50. doi: 10.1109/ISBAST.2014.7013092.