Security and Efficiency Based Identification of Biometric Data File in Cloud Computing

Mr. Suresha D[2], Pooja Deshpande[1]
[1]Student, Department of CSE, Dr. Ambedkar Institute of Engineering and Technology, Bengaluru, India
[2]Associate Professor, Dr. Ambedkar Institute of Engineering and Technology, Bengaluru, India

Abstract: Biometric is the term that alludes to person attributes, gives the estimations and computation of a human body. Securing information has been a focused undertaking since years. Biometric information has turned into a requested security for one's recognizable proof and confirmation. Advanced technologies like cloud computing provoked database owners to unload the large size of biometric data and identifying tasks to the cloud to exterminate expensive storage and computational costs, which will surely bring optimistic threats to user's privacy. The boundless appropriation of biometric data requires strong security assurance against possible misuse, loss, or theft of biometric data. Existing methods for security preserving biometric data essentially depend on customary cryptographic natives, for example, homomorphic encryption and oblivious exchange, which definitely acquaint huge expense with the framework and are not relevant to practical large scale applications. This paper proposes efficient scheme with different levels of security to protect Biometric data in cloud computing. Particularly, to implement Biometric identification, the database proprietor encrypts the data and outsources it to the cloud server. By encrypting the data which will then be appearing in a cipher-text form and then eradicating it to the cloud will preserve user privacy and efficiency of storage also increases. The cloud server will then execute the identification process with the encrypted data sent by the data owner and send back the result to the database owner. A broad security investigation or in-depth estimation states that proposed plan is secure against malicious users or attackers who can forge identification requests and converge with the cloud.

Keywords: User, Data Owner, Cloud Server, Security, Efficiency, Biometric Identification.

I INTRODUCTION

Biometric identification has turned out to be impressively famous among numerous clients since it gives a trust commendable approach to distinguish clients and secure clients Biometric information through various dimensions. Biometric identification strategy is been increasingly reliable; trust commendable and easy to understand when contrasted with moderate verification techniques that is depended on password protection and identification cards. Nonetheless, Biometric identification arrangement has been massively practiced in various zones utilizing biometric properties, for example, finger print, facial patterns and iris, which can be assembled through different sensors. Biometric gives the estimations and count of a human body. Biometric information has turned into a requested security for one's distinguishing proof and confirmation. It can drastically build the venture security.

In this plan of identification database proprietor/owner will be in charge of holding the clients biometric information and would then be able to want offloading the information onto the cloud server to reduce expensive capacity and computational expenses. Here client's security is kept up by encrypting the information before offloading the information to the cloud server. At whatever point an approved client needs to download biometric information then the solicitation/request would be sent to the database proprietor who at that point reacts to a solicitation/request made by the client. In this manner, the energizing issue here is to distinguish a convention which gives both efficiency and protection of biometric identification in cloud computing.

In a method for improvement the vast majority of them focus on security and disregard the effectiveness or efficiency, for example, schemes dependent on homomorphism encryption, unique finger impression and face picture distinguishing proof individually. These plans don't give efficiency once the size of the database increments.

This paper proposes efficient and security-preserving scheme for distinguishing biometric information in cloud computing which can oppose the collusion attack started by the clients and the cloud.

Our fundamental grants can be sketched out as follows:

1) Examining of biometric data identification plan is done where its inadequacies and security foible is appeared on how the malicious attacker can attack and connive with the cloud and recover the clients information.
2) Presentation of a peculiar secure and efficiency based biometric data identification strategy. This gives a thorough survey on privacy-preserving strategies that can accomplish a required dimension of security. This plan is secure and effective to oppose any attack created by the malevolent user.
3) Performance of this plan likewise gives the more prominent outcomes by bringing down the computational expenses in identification procedure in correlation with the current biometric data identification schemes.

This paper presents efficient and secure scheme with different levels of protection for distinguishing Biometric information in cloud computing. Curiously, to show Biometric identification, the database proprietor/owner encodes the information and submits it to the cloud server. Here client's security is kept up by encrypting the information before offloading the information to the cloud server. The cloud server will perform identification procedure utilizing encoded information and returns the outcome back to database proprietor/owner.

The following situation shows how the client's security is kept up with efficiency.

Consider Alex is a client who wishes to secure his biometric information in cloud storage and needs to access to that information at whatever point he require. First Alex needs to enroll as a client by giving a first dimension of security that is by giving his biometric distinguishing proof. He will be in a waiting to be authorized state until the cloud server approves him as a trust-worthy user. When

this is done Alex can login and do the required download or transfer activities at whatever point required. The transferred biometric information by the Alex will at that point be sent to the Data Owner where he will acknowledge the solicitation and contact with the cloud server to store the information safely. This is done because it will wind up complex if the information transferred by the Bob increments. At the point when Bob needs to download the information that was transferred beforehand He will be furnished with the secret key which ought to be matched to get the requested query.

II RELATED WORK

This section provides few related works on security based biometric identification scheme. Below are few works on efficient biometric identification scheme. Wang and Hatzinakos propose a secure face-recognition scheme [1]. Specifically this work is done by calculating the similarities among sorted index numbers vectors. Wong and Kim [2] introduced secure biometric identification protocol using iris code verification. In their work, it is measurably inaccessible for a malevolent user to impersonate as an authorized user. Barni *et al*. [3] proposed FingerCode matching strategy based on the Homomorphism Encryption technique. Nevertheless, in this database every distance are calculated between query and sample FingerCodes which can in turn produce large amount of burden as the size if the finger prints raises. In concern with efficient storage, Evans *et al*. [4] proposes a work that decreases the matching time. They used improved Homomorphism encryption algorithm to execute the Euclidean distance and designed a related garbled circuits to get the less distance. By utilizing a backtracking protocol, the best match FingerCode could be found. However, [4] the whole encoded database must be transmitted from a database server to the client. Wong *et al.* [5] proposed an identification scheme on kNN to acquire a protective search in the encoded database. However, their identification schemes surmise that there is no collusion attack between both cloud server side and client side. Yuan Yu [6] introduced an efficient privacy-preserving biometric identification scheme. Although [11] it is said that the convention can be attacked if the malevolent user colludes with the cloud server in biometric matching procedure. Wang *et al* [6] presented a privacy-preserving biometric identification in [7] which it will introduce random diagonal matrices named CloudBI-II. However, it is not efficiently secure in [8] and [9]. Not long ago, Zhang *et al* [10] introduced an efficient and privacy-preserving biometric identification scheme which then uses fazed idioms.

III PROPOSED WORK

Proposed framework is secure and efficient biometric identification strategy which can oppose the collusion attack propelled by the malicious assailant, clients and cloud. First the adequacy level and security insufficiency of biometric data identification plan are analyzed and appeared under a level 2 attack. In an exhibition it is demonstrated that how a malicious user can recover the secret key given to the client by colluding with the cloud and afterward decrypt all the biometric information of the clients. Proposed work gives secure and efficient biometric data identification scheme with various levels of security.

As appeared in Figure.1, three kinds of individuals are associated with the framework including the database proprietor, clients and the cloud server. The database proprietor holds a huge size of biometric information which is encrypted and transmitted to the cloud for capacity. At the point when a client needs to recognize him/her, a query solicitation/request is being sent to the database proprietor/owner. In the wake of getting the solicitation, the database proprietor creates a cipher-text for the biometric quality and after that transmits the cipher-text to the cloud for data identification. The cloud server figures out the best match for the encrypted query and returns the related record to the database proprietor. At long last, the database proprietor computes the similitude between the inquiry information and the biometric information related with the index, and returns the query result to the client.

Cloud Server exhibits a prominent role where the information of the client is stored and can be recovered whenever. Apart from this it should also guarantee the security of the client's information which could be attacked by the malicious clients.

Data Owner acts as a middle person between the client and the Cloud Server as it will acknowledge the information and the solicitations from the client and contact with the cloud server to give the expected result to the client. These are the main functionalities of the Data Owner.

Client who needs to preserve security to their Biometric Data contacts with the Data Owner. Client will then be allowed to download the requested data. Client can Upload the information; download the information and login with the approved and authorized credentials to do every required operations.

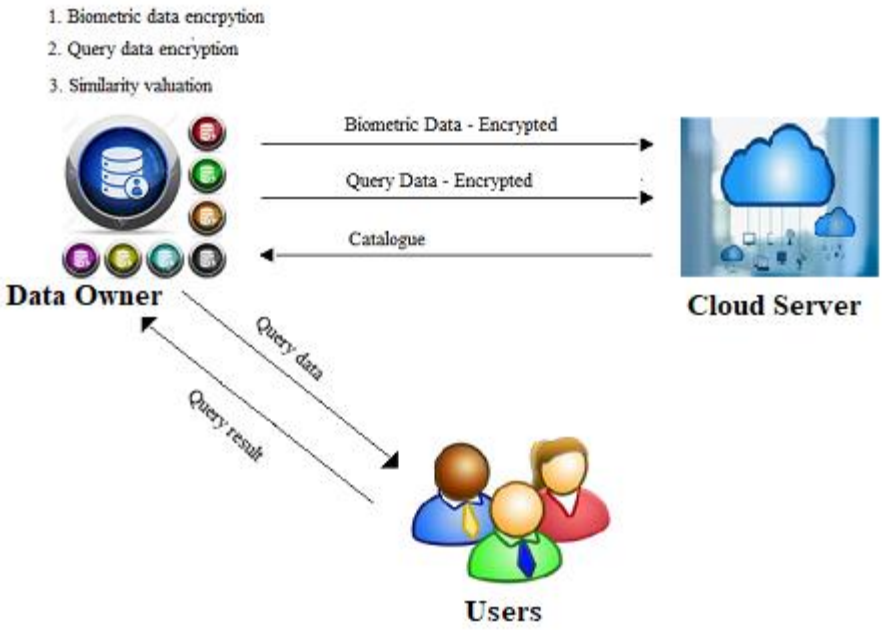

Fig-1: System Architecture

Above mentioned three entities play important role in the project with their specific functionalities.

Algorithm steps:

Below are the steps that explain HMAC algorithm description and use to provide the efficient security level.

Key Generation:

1) Make the length of K equal to b.
2) XOR K with Ipad to produce S1.
3) Append M to S1.
4) Message-digest algorithm.
5) XOR K with opad to produce S2
6) Append H to S2.
7) Message-digest algorithm.

Step 1: Messages/Data communicated between data owner and the servers are encrypted/decrypted by RSA public and private keys.

Step 2: In RSA encryption, one will be given with a key called public key which is shared transparently among user which is then used to encrypt the messages.

Step 3: Because of some well-defined mathematical properties of the RSA calculation, whenever a message is encrypted using a public key, it must be and can be decrypted using a secret key called private key.

Step 4: Every user to use RSA encryption should have both public key and private key. As the name implies the private key of a user must be kept as a secret.

Step 5: Public key encryption and symmetric-key encryption are both different schemes, where the symmetric-key encryption uses same private key to both encrypt and decrypt.

Step 6: These distinctions make public key encryption like RSA valuable for imparting in circumstances where there has been no chance to securely disseminate keys in advance.

Step 7: Data owner biometric images are stored in the database and they are allowed to access after successful submission of the secret key.

Step 8: The secret key will be distributed by the cloud admin server to end user or data owner once they are authorized.

Advantage of proposed system:

- More security, Reduce workload and enhance productivity with better flexibility and speed.
- **Efficiency:** Computational expenses ought to be as inexpensive as conceivable for both the database proprietor and client. To increase more efficiency, most biometric data identifying tasks ought to be performed on the cloud.
- **Security:** During the matching procedure, security of biometric data is ought to be ensured. Assailants and the semi-genuine cloud ought to get the hang of nothing about the delicate data.

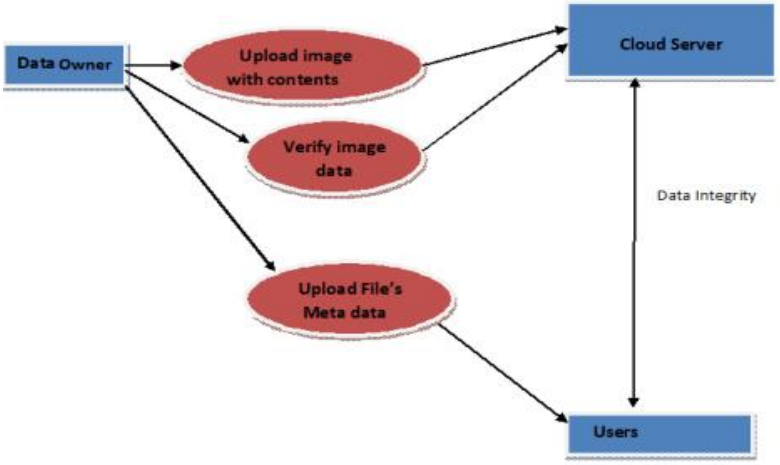

Fig-2: Dataflow Diagram

Figure 2 above portrays a framework as far as input information to the framework, different processing carried out on this information and yield information produced by this framework.

Cloud Server performs a prominent role where the information of the client is stored and can be recovered whenever. Apart from this job it guarantee the security of the clients information which could be attacked by the pernicious clients.

Data Owner acts as an mediator between the client and the Cloud Server as it will acknowledge the information and the solicitations from the client and contact with the cloud server to give the expected result back to the client. These are the prominent functionalities of the Data Owner.

User/Client who needs to preserve the security of their Biometric Data contacts with the Data Owner. Client can Upload the information; download the information and login with the approved and authorized credentials to do every transactions.

IV RESULTS AND DISCUSSION

Results an efficient and security-preserving plan for recognizing biometric information in cloud computing which can oppose the collusion attack initiated by the clients and the cloud. This introduces a novel secure and efficient biometric identification scheme. This detailed privacy-preserving approaches that can accomplish a required dimension/level of security. This scheme is secure and effective to oppose any attack delivered by the vindictive attacker.

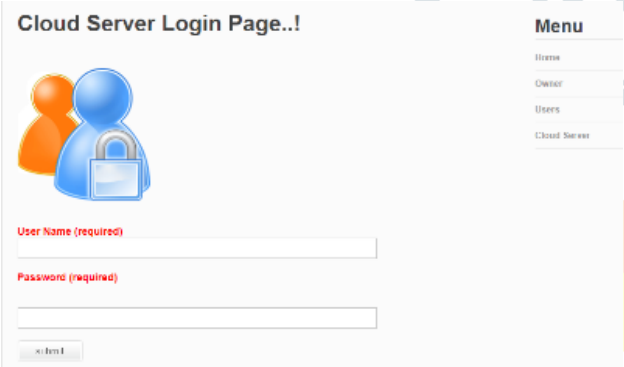

Fig-3: Cloud Server Login

Figure 3 above depicts the cloud server login and the options available.

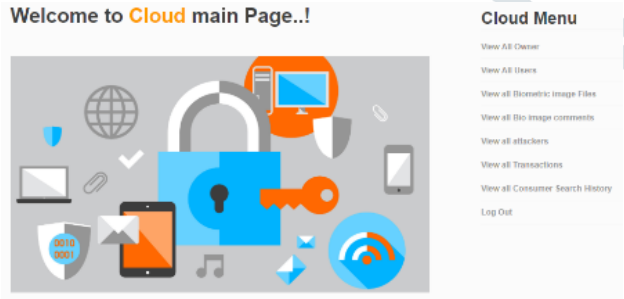

Fig-4: Cloud Server after Login

Figure 4 above depicts the menu options that are available for Cloud Server and the It can perform all the given options.

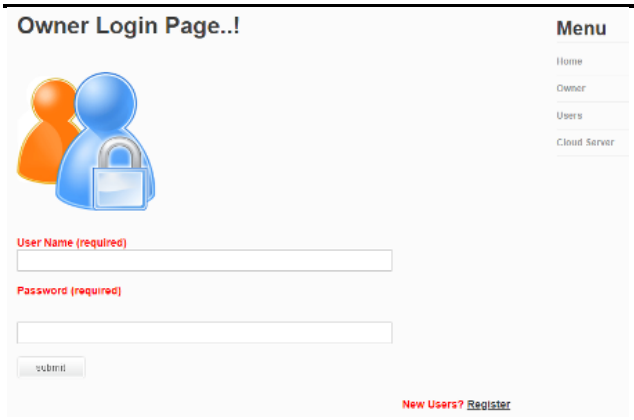

Fig-5: Database Owner Login

Figure above depicts the login page of a database owner who would be responsible for accepting the requests from the user.

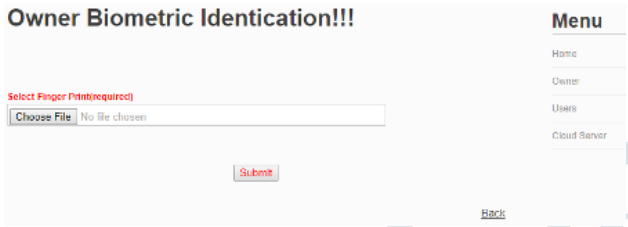

Fig-6: Identification proof to Login

Figure above depicts that after a successful entry of a database owner credentials one should also provide his/her biometric identification where the matching will be for future login.

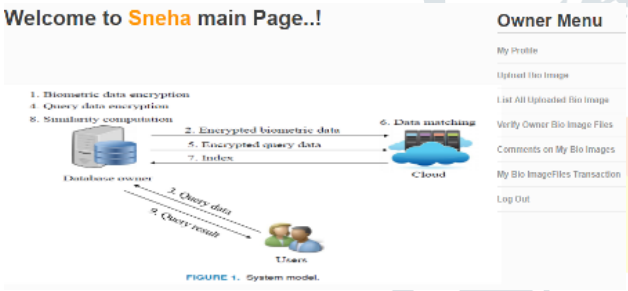

Fig-7: After Owner Login

Figure above depicts all the options available for a database owner after a successful login by providing required credentials. Data owner can then perform the operations and respond to the user's request.

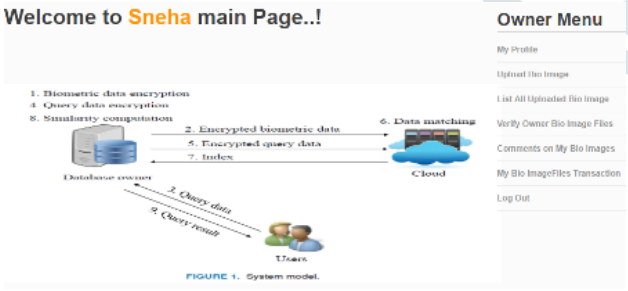

Fig-7: Operations after User Login

Figure above depicts the available option after a successful register and login of the trusted user. User can perform all the operations like download and upload. But after a new user login he/she will be in a waiting state where the cloud server will then authorize the user.

Fig-8: To download Biometric image

Figure above depicts the conditional credential that must be entered by the user to download the biometric image.

Fig-9: To upload Biometric Image

Figure above depicts the credentials that must be entered by the user to upload a Biometric image. A normal text file has to be created have two lines of a description about the uploading image.

Fig-10: Encrypted form of credentials

Figure above depicts that once the user enters all the required credentials which is then verified the next step it does is it encrypts all the information that was provided by the user to have level of security and hence the user feels safe about the data that was uploaded. Encrypted data would not be attacked by the malicious user because it would be difficult to breach the security and decrypt the data.

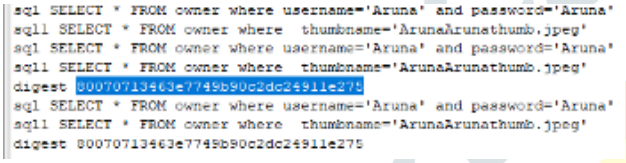

Fig-11: Master Key generated for each owner

Figure above gives the description of a generated key for each owner. It would be a master key which gets generated for each owner when the image gets uploaded.

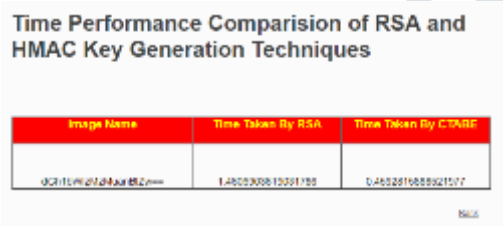

Fig-12: Time or speed performance

Figure above gives the description of time required to upload the image, retrieve the image, generate the key and encrypt the information

This paper proposes a novel secure and effective Biometric Identification scheme in cloud computing by giving different levels of security. The definite examination and results demonstrates that it can oppose potential attack done by any pernicious client or assailant. Performance and efficiency likewise give the great outcomes as it utilizes a cloud to store the biometric pictures which would then be able to be recovered by the client at whatever point required. Information entered by the client alongside the credential information will be encrypted that can't be attacked by the malicious client consequently clients can have a more noteworthy trust and store the Biometric information on to the cloud.

In this way the conclusion here express that Information entered by the client to the cloud has dimensions of security and can be trusted to be safe.

Hence it can be further enhanced where Secure and Efficient Identification of a Biometric Data in cloud computing is secure through various and more dimensions of security and effective through storing information onto the cloud that avoids the storage complexity to the user and makes the users life easier.

REFERENCES

1. Y. Wang and D. Hatzinakos, "Face recognition's with enhanced privacy protection", in Proc. IEEE Int. Conf Acoust., Speech Signal Process., Ap. 2009, pp.885-888, 2009.
2. K. Wong, and M. Kim, "A privacy-preserving biometric matching protocol for iris codes verification," in Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), pp. 120-125, 2012.
3. M. Barni, T. Bianchi, D. Catalano, et al., "Privacy-preserving fingercode authentication," in Proceedings of the 12th ACM workshop on Multimedia and security, pp. 231-240, 2010.
4. D. Evans, Y. Huang, J. Katz, et al., "Efficient privacy-preserving biometric identification," in Proceedings of the 17th conference Network and Dis- tributed System Security Symposium, NDSS, 2011.
5. W. Wong, D. Cheung, B. Kao B, et al., "Secure kNN computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD Interna- tional Conference on Management of data, pp. 139-152, 2009.
6. J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in Proc. of IEEE INFOCOM 2013, pp. 2652-2660, 2013.
7. Q. Wang, S. Hu, K. Ren, et al., "CloudBI: Practical privacy-preserving out- sourcing of biometric identification in the cloud," in European Symposium on Research in Computer Security, pp. 186-205, 2015.
8. Y. Zhu, Z. Wang and J. Wang, "Collusion-resisting secure nearest neighbor query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.
9. S. Pan, S. Yan, and W. Zhu, "Security analysis on privacy-preserving cloud aided biometric identification schemes," in Australasian Conference on Information Security and Privacy, pp. 446-453, 2016.
10. C. Zhang, L. Zhu and C. Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol. 409, pp. 56-67, 2017.
11. Y. Zhu, T. Takagi, and R. Hu, "Security analysis of collusion-resistant near- est neighbor query scheme on encrypted cloud data," IEICE Transactions on Information and Systems, vol. 97, no. 2, pp. 326-330, 2014.
12. A. Jain, L. Hong and S. Pankanti, "Biometric identification," Communica- tions of the ACM, vol. 43, no. 2, pp. 90-98, 2000.
13. R. Allen, P. Sankar and S. Prabhakar, "Fingerprint identification technol- ogy," Biometric Systems, pp. 22-61, 2005.
14. J. de Mira, H. Neto, E. Neves, et al., "Biometric-oriented Iris Identification Based on Mathematical Morphology," Journal of Signal Processing Sys-tems, vol. 80, no. 2, pp. 181-195, 2015.
15. S. Romdhani, V. Blanz and T. Vetter, "Face identification by fitting a 3d morphable model using linear shape and texture error functions," in European Conference on Computer Vision, pp. 3-19, 2002.
16. Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.