ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

BIOMETRIC IDENTIFICATION SCHEME WITH EFFICIENT PRIVACY-PRESERVING MECHANISM FOR CLOUD COMPUTING SERVICE

[1] Tsks jyothirmayi,[2] Gora Harika, [3] Sabavath Raju, [4] Eedunuri Muralidhar Reddy

[1,2,3,4] Assistant Professor, Department of Computer Science Engineering,

Pallavi Engineering College, Hayathnagar_Khalsa, Hyderabad, Telangana 501505

Abstract: People are using lot of cloud storage service (CSs) to store various types of information. The cloud storage services are used to conserve people personal data and facilitate data transferable. The computer which connected via internet is adequate to access the data anywhere without carrying any physical drives like Pen drive, CD, etc. In existing techniques like, CSs providers are using 256-bit Advanced Encryption Standard (AES) and 128-bit (AES) encryption algorithm. This is one of the best techniques to secure data, but once the intruder gets encrypted data, there is possibility for data insecurity by means of applying brute force attacking technique in future increasing the speed performance of computer. The objective of this paper to implement the Privacy Preserving Biometric Authentication and Identification based cryptographic algorithm which perfume on various data formats and to reduce data security attacks and threads in cloud storage environment. The aim to overcome this kind of attacks and key tampering technique, the key generation and maintain process handover to user's itself. It makes cloud storage service provider to maintain data only, with high efficient encryption technique that provides strong protection for data. The simulation results shows that the proposed method gives the better authentication and security compared to the state of art approaches.

KEYWORDS: cloud storage services, cryptography, security, multifactor authentication.

1. INTRODUCTION

In cloud storage and computing environment data privacy and its security are the major concern. To overcome this concern, we fuse cryptography concepts into cloud computing. Cryptography help in data encryption and decryption procedure is use to protect the data in cloud. To ensure privacy, data encryption is done by the user. The user share the file through cloud but person who knows the key only can decrypts the file [1]. The intruder gets the file but they can't decrypt. In evolution process, intruder try to crack the key using look up table technique, brute force technique etc. The traditional security methods are not masterly enough to manage the cloud specific threats. The enhancement of the key building concepts which plays vital role in

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

data security in cloud computing. By generating type of keys are public key and private key [2]. In later part technology developed and advance concepts make the encryption process with hashing techniques. Using hashing techniques the key was hashed with salt, now users itself don't the key after the hashing. On go through process user enter the key for decrypting the file. Initiation decryption, first key was hashed with salt in background process. The output of hashed key will be executed in the decryption process[3].

Finally, the evolution process of encryption algorithm: algorithm itself generate the round keys in fusion of master key which given by the user. These techniques are used to secure data in cloud environment.

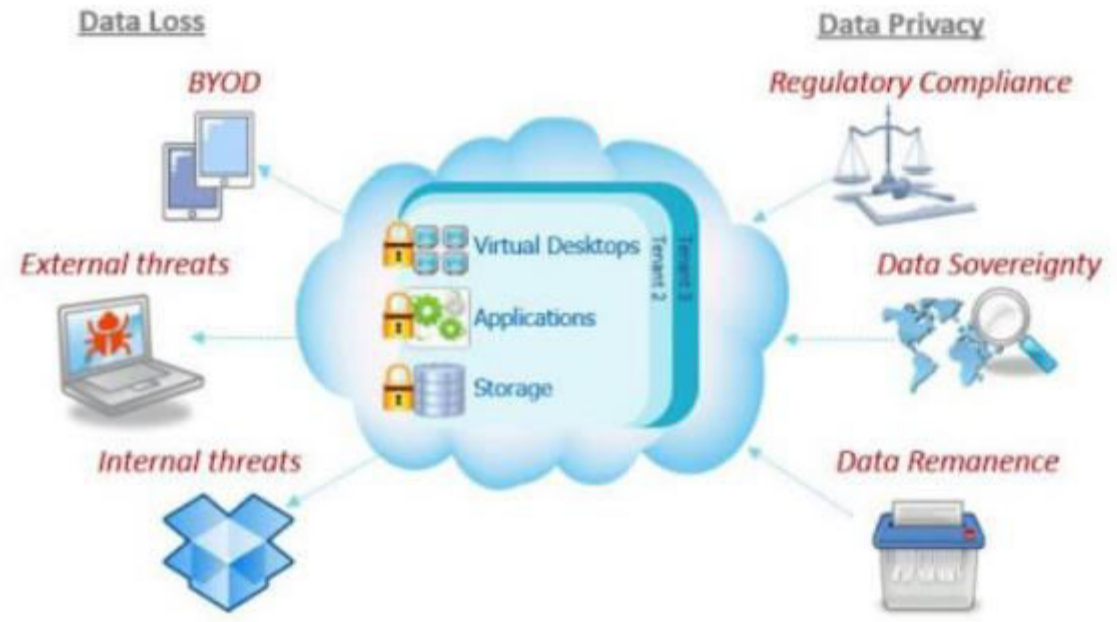

FIGURE 1: Cloud storage data security threads

In a biometric identification system, in this model, virtualized infrastructure is offered to cloud users [4]. The consumer will tells the required software system as Operating System and applications packs all of along into virtual machines (VMs).Hardware demand the Micro Systems to adjust the customer. Finally, the VM is host into the environments controlled by third-party suppliers. A cloud provider gives the guaranty of the standard of service for running VMs. Where the cost of computing is maintained and managed by supplier. Biometric authentication has raises progressively attended since it's provided a promised method to identify the users and compares with the ancient authentication plan [5]. This is the most using method now a-days. In which the Computing resources are processing power, power supply, storage

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

disks, and software to use and networking information measure, are described to all cloud using customers because of the accessibility services (IaaS) Infrastructures-a-Service [6].

The fingerprints may be extremely good lines in groups of people as not individual shares identical fingers print. Therefore it's a really solids a proofs-of-characteristics for the identities of individual users whereas activity authentications. The fingerprint pattern are known mistreatment sub- characteristic like crossovers, core, bifurcations, ridge endings, islands, deltas, pore etc. the foremost drawback of fingerprints as Associate in Nursing authentications is that the aspect of skin. In this model, virtualized infrastructure is offered to cloud users [7]. The consumer will tells the required software system as OS and applications packs all of along into virtual machines (VMs).Hardware demand the MS to adjusts the customer. Finally, the VM is host into the environments controlled by third-party suppliers. A cloud provider gives the guaranty of the standard of service for running VMs. Where the cost of computing is maintained and managed by supplier. BIOMETRIC authentication has raises progressively attended since it's provided a promised method to identify the users and compares with the ancient authentication plan. And this is the most using method now days [8].

In above figure illustrating that what are the threads and issues are facing by the cloud storage. Here clearly defining the internal threats, external threats, shared technology vulnerability, etc. that says whatever the data stockpile in cloud storage by people is already in high risk state [9].

The major contributions of this work as follows:

- Data acquisition, this is the stage in which data (fingerprint) is acquired through a User interface. The obtained image is stored in database.
- The functions of finger prints are extracted and saved at the side of its info in the gadget database. When the fingerprint photos are fed to feature extraction module, a characteristic extraction set of rules is first implemented to the image and its capabilities are extracted .The proposed system consists of SVD (Singular Value Decomposition) based feature extraction.
- Then the features are matched with the database and provide the matched results.

This paper is summarized follows through as: In Section 2, literature review for cloud data security with the comparison of methodology with defining problem, implication, merits and demerits. Section 3 gives the detailed information about the proposed methodology. Section 4

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

discusses about the results analysis and finally Section 5, concluded the summarization of whole paper.

2. LITERATURE REVIEW

S. Atiewi et al., (2020) abstracted an IOT based multifactor authentication and light weight cryptography encryption scheme in cloud storage environment. IOT device are organize as follow of sensitive data and non-sensitive data. The sensitive data is split in two and each part encrypted by separated encryption algorithms (RC6, Fiestel) and data deposit on private cloud storage to ensure the high security. Non-sensitive data is encrypted by single algorithm (AES) as stored in the public cloud. Multifactor authentication ensure through the trusted authority. Using the identification of user's such as IP, password and biometrics in [10].

X. Wang and Y. Su (2020) proposed a new encryption method for audio which dispense reliability state high. Preliminary value that presents in chaotic controlled by hash value on the audio and then making unpredictable chaotic trajectory, DNA coding is used to mystifying and scatter the data (audio). Encryption scheme is used for single and dual format audio [11].

D. Changet al., (2020) illustrated a cancelable multi-biometric approach by fusion of fuzzy extractor with a novel bit-wise encryption scheme to engender cancelable biometric templates. The protection scheme for biometric template framed as irreversibility, renewability and accurate recognition of biometric scenes. The scheme that safeguard without supplementary noise that means of bit errors is executed in preserved template [12]

F. Shahidet al., (2020) stated new scheme for data Security with less complexity. Proficient security our distributed storage concept divided the data as sensitive along with normal part. The data specified as normal, separately encrypted after saved in single storage cloud but the sensitive in seriated as dual portion, the encryption process done separately and stored in different cloud. This proposed method is used to secure against following attack, related key attack, man-in middle attack, pollution attack in [13].

J. Zheng and L. Liu (2020) proposed 2D chaotic system is fusion of sine maps along with logistic map. The sine map makes on combination of two chaotic maps. Now, new encryption design for a dynamic DNA encoding and decoding. Using this algorithm achieved security test, they are key sensitive, histogram and correlation analysis. It makes difficult for most successful attacks in [14].

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

Y. Zhang and B. Li (2020) conducted neuron-like scheme, masking operation, flipping operation for image cryptographic algorithm. The neuron-like based learning scheme makes to identify a catchy scattered scheme and execute the plaintext based image encryption algorithm. The process gets input and weights of the neuron through the feedback operation to regulate the information of image. Finally, the encryption algorithm which makes to scatter the image data. It results high security and adaptive characteristics in [15].

H. Hu, et al., (2019) Identified intruder can intrude any important information on mode of transfer. To rectify an issues by encryption process done before the transmit data for cloud storage. For protection of hidden encryption password, designed hidden transmit mode along with multi authority factor. First user split a hidden password which makes encrypt important file splits trivial parts. Then user use the own key along with biometrics to conceal a hidden password parts [16].

Y. Song et al., (2019) evolved novel based key substitution encryption algorithm purpose a progressing key for upgrade the commencing keys implement plain image and evolve another substitution scheme that encrypting different category images. It helps to overcome the low security and low computational that apply uses single round encryption only. The proposed substitution method which establish on s-boxes to different categories image encryption [17].

W. I. Khedr et al.,(2019) CAPDP allows storage user to do data integrity verification infinite. The verification process is self-reliant of the count of blocks being checked in [18]. W. Feng, et al., (2019) [19] enhance the hash value which used in the plain image during encryption activity makes unworkable for intruder to deploy of special plain-image attack. DNA encoding and decoding schemes invoke plain image correlated DNA order progress further dependent on hashed data.

H. T. Poon and A. Miri (2019) abstracted technique used phrase search based Bloom filters in [20]. It uses services of n-gram filters to adopt functionality. It allows phrase search to execute self-sustain without initial progression of conjunctive keyword based search that detect user files.

H. Lin (2019) discusses pre-authentication and post authentication of user to avoid anonymity. In this scheme administrator assist the user to generate the pseudo identity which is known to the user. Using the pseudo identity administrator registering in cloud servers and it help to verify user's authentication of requesting client. This technique is very useful trace the illegal user. This protection support fast error detection or offline password update [21].

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

A. A. Pammu et al., (2019) Proposed matrix transformation based on authentication and parallel encryption implemented on multi-core processor. It helps to active high through put, comprehension performance and secure AES construct on counter with chaining mode [22]. W. Luo et al., (2019) Introduced new password protect which desires from plaintext password to hashing password, hashing password, to negative password and finally using symmetric-key algorithm for creation encrypted negative password. They conclude technique is secure from lookup table attack as dictionary attacks [23].

3. Proposed Methodology

Biometric authentications refer to the identifications of humans by their Physical characteristic are behavior trait. Bio- metric authentications typically support three main factors that are identifications, authentications and non-repudiations that are employed for characteristic the physicals and also the behavioral attribute of the people. This authentication has replaced the standard type that use the crypto logical technique supported keys. Identity verification is static authentication systems wherever the persons are going to be verify at the beginning of the processes itself. The identity verification itself has been classifies broadly speaking into the Physical Biometric technique and also the behavioral biometric methods. In figure 2 represent the fingerprint pattern. The finger prints may be extremely good lines in groups of people as not individual shares identical fingers print. Therefore it's a really solids a proofs-of-characteristics for the identities of individual users whereas activity authentications.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

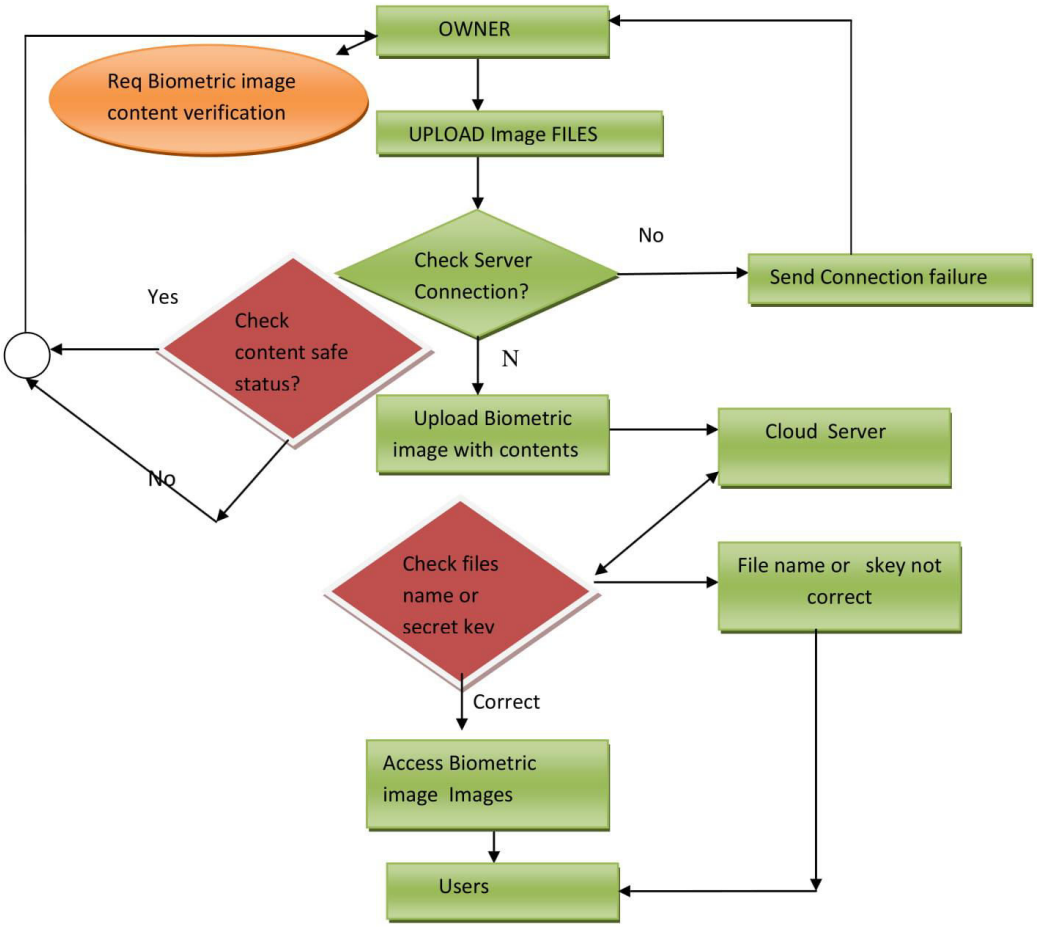

Figure 1: Flowchart of proposed method

The fingerprint pattern are known mistreatment sub-characteristic like crossovers, core, bifurcations, ridge endings, islands, deltas, pore etc. the foremost drawback of fingerprints as Associate in Nursing authentications is that the aspect of skin surfaces like waterlessness, condition will considerably have an effect on the standard of the fingers print authentication.

Data acquisition: This is the stage in which data (fingerprint) is acquired through a User interface. The obtained image is stored in database.

Feature extraction: In this article the functions of finger prints are extracted and saved at the side of its info in the gadget database. When the fingerprint photos are fed to feature extraction module, a characteristic extraction set of rules is first implemented to the image and its capabilities are extracted .The proposed system consists of SVD (Singular Value Decomposition) based feature extraction.

Proposed Algorithm is Biometric authentication and identification.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

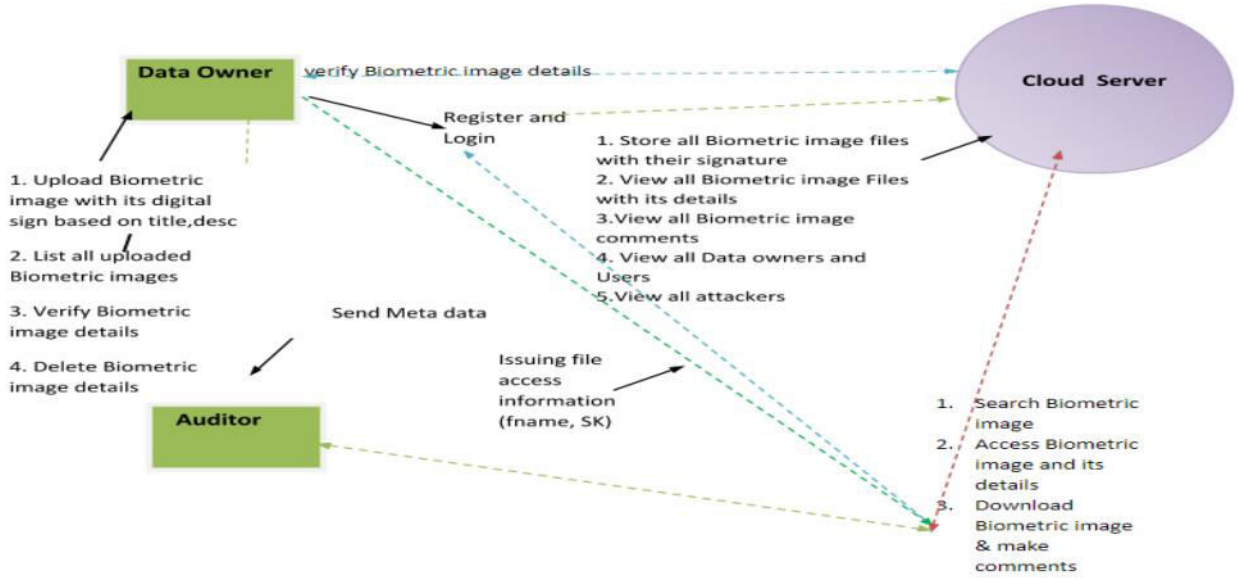

Figure.3. Biometric authentication and identification algorithm

In figure 3 represent the work flow of the proposed algorithm. Here this proposed work shown the step by step processor.

A. Registration Process:

Step-1: A contactless acknowledgment framework checks (read) minutiae (where edges of fingers and lines end or edges split in two) from fingers and wrinkles from palm (computerized palm print acknowledgment framework).

Step-2: from examined finger prints, a hash code is produced and put away to the diverse databases.

B. Verification:

Step-1: Scans minutiae from fingers through an optical sensor.

Step-2: After the checking procedure, a hash code is produced from examined biometric.

Step-3: Comparison between the hash code of newly obtained fingerprint and hash code of fingerprint which is already stored is performed. I. On the off chance that hash codes are not coordinated, the demand of check is dropped. ii. Else verification process is finished.

Step-4: Enrolment: This step prepares the smartcard for use and pairs the person with the card. A reference sample, such as a fingerprint or a sample of writing is taken. The reference sample, called a template, is stored either in a database, managed by the authenticating authority, or on the card itself.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

Step-5: Livesample: with the template in place, the smartcard is now ready to use. Each time the card is put to work, the user provides a live version of the reference sample (a fingerprint or a handwritten PIN code) as part of the authentication process. The sample can be taken by the card itself, or by a machine that interacts with the card. Either way, the next step, comparison, is usually performed on the card.

Step 6: Comparison: To complete authentication, the live sample from step 2 is compared to the reference sample in the template. If the live sample is verified to be a match with the template, then the smartcard is authenticated and the transaction can proceed.

4. Results and Discussions

For performing the experiments the FVC 2018 databases is considered with 1000 train images and 100 test images. Even although the authentication is executed and cloud get entry to be granted to the person the records had to be decrypted so as to get original facts. If the given or considered fingerprint or palm print does not fit the records decrypted will also goes incorrect and raw information will no longer be uncovered to no one except the proprietor of that data. Multimodal biometrics are now cherishing than any single biometric system authentication. So, the combination of finger print and palm print gives us a great combination.

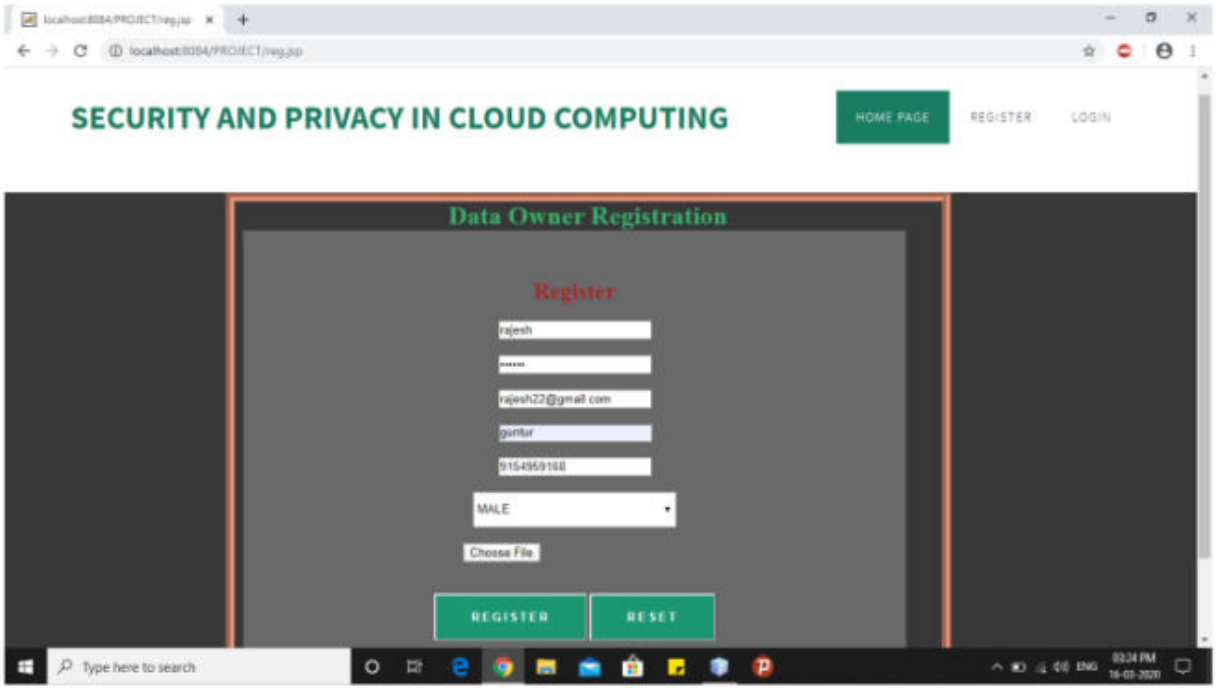

Figure: 4 Data owner registration in proposed system

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

In figure 4 shown; the registration process is very simple and clear. The user has to enter his details which are required; user has to enter his username, password, mail-id, and his location. Here there is an option choose file where the user has to upload biometric fingerprint to the place. Once user has done all can click register. He will get register or else user had an option reset and again can change the details which he wanted to before he get registered. User may not be allowed to change the data after registration. After registration the details of the user will be sent to the admin. Admin has to activate the users' account which he wanted to activate.

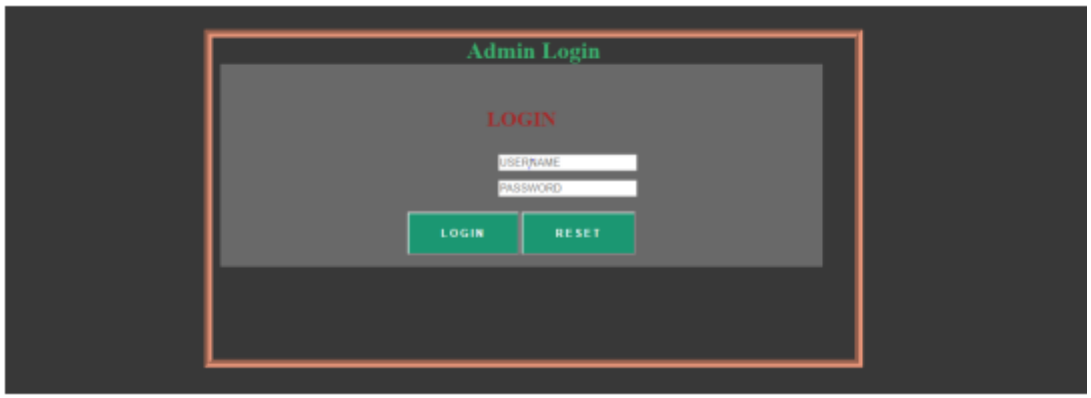

Figure: 5 Admin login page

In figure 5 shown the admin login process; Once the user will register then the admin will login and activate the account for that user then the user will login the own page if the admin will not activate your account the user doesn't allow for the login once you will login then your files can upload for the security we can provided.

After the activation of the account the user can login to his account and he can upload the files which he wanted to be secured .After user login to his account he will upload the file while uploading the file he need to give his finger print copy .The finger print which user is giving while uploading the file should match the finger print while given on registration time. The file will be more secured only user can access that account. When he is in need of that file, he opens his account and go to uploaded files and opens it.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

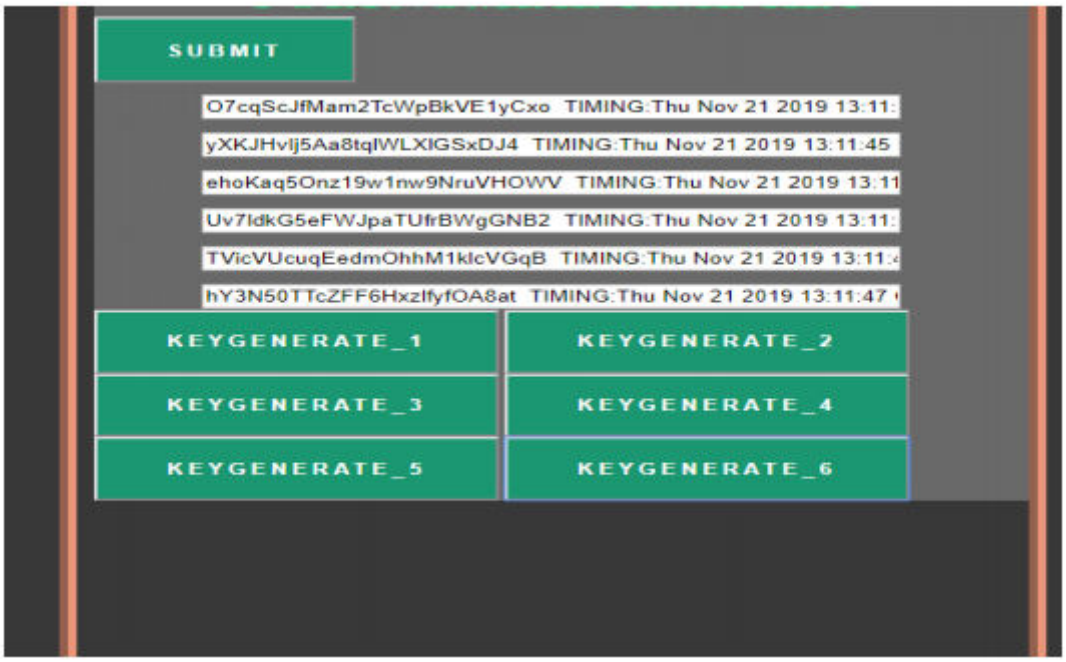

Figure 6: Different Key generations in proposed system

In figure 6 shown the different key generations, in emergency the user may want the file to be downloaded, so that the user need to login account and go to file downloads .When user clicks the file download then it asks for the unique key for the generation of the file to be downloaded. In back end there will be generated 5 different keys by the polynomial time algorithm which helps to generate the unique key with the help of Diffiehellmen process. After the unique key generation we can get that key from the data base, we use that key and we could download the file. Thus our article helps our clients to secure their personals in our infrastructure safely.

5. CONCLUSION

In this Article report, we tend to propose efficient and privacy conserving biometric identification theme in cloud computing. This biometric identification technique is one in all the foremost secure and new rising strategies in cloud computing. To fulfill the efficiency and security needs, we tend to had designed a brand new coding rule and cloud authentication. This careful analysis shows that it will resist the potential attacks. Besides, performance this biometric identification provides higher security from the attackers and malicious code. Therefore the user will safely store the info, send the info, and may transfer the info with none hurdles and changes of information. This method is a use full method to securely safe our data from the attackers and this is a most secure effective method of encrypting the data for the better security of the user

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

and which help the customer can trust a online cloud computing service provider that they can safely put his/her data in a cloud for all dangerous attacks.

This literature survey centered on the varied biometric authentications technique that are a accustomed manifest user in cloud computing. It's an evident that among the authentications technique, the standard ways like password, OTP, positive identification token etc. have an explicit variety of draw back in making certain the genuine of the users UN agency is to be authenticated. Hence, biometric technique are thought about to better than typical ways in facilitating secures and valid authentications in cloud computing. We have additionally created comprehensive studies of most of the key biometric technique that are present obtainable.

REFERENCES

1. Q. Zhang, J. Han and Y. Ye, "Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding," in IET Image Processing, vol. 13, no. 14, pp. 2905-2915, 12 12 2019, doi: 10.1049/iet-ipr.2019.0667.
2. H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," in IEEE Access, vol. 6, pp. 26059-26068, 2018, doi: 10.1109/ACCESS.2018.2832854.
3. J. Howe, A. Khalid, C. Rafferty, F. Regazzoni and M. O'Neill, "On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography," in IEEE Transactions on Computers, vol. 67, no. 3, pp. 322-334, 1 March 2018, doi: 10.1109/TC.2016.2642962.
4. Y. Liu, Q. Zhong, L. Chang, Z. Xia, D. He and C. Cheng, "A secure data backup scheme using multi-factor authentication," in IET Information Security, vol. 11, no. 5, pp. 250-255, 9 2017, doi: 10.1049/iet-ifs.2016.0103.
5. Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu and X. Zhang, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676-688, March 2017, doi: 10.1109/TIFS.2016.2631951.
6. K. Bai and C. Wu, "An AES-Like Cipher and Its White-Box Implementation," in The Computer Journal, vol. 59, no. 7, pp. 1054-1065, July 2016, doi: 10.1093/comjnl/bxv119.
7. J. K. Liu, K. Liang, W. Susilo, J. Liu and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," in IEEE Transactions on Computers, vol. 65, no. 6, pp. 1992-2004, 1 June 2016, doi: 10.1109/TC.2015.2462840.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

8. H. D. Nguyen and K. Turitsyn, "Robust Stability Assessment in the Presence of Load Dynamics Uncertainty," in IEEE Transactions on Power Systems, vol. 31, no. 2, pp. 1579- 1594, March 2016, doi: 10.1109/TPWRS.2015.2423293.
9. D.Godwin Immanuel, Dayana D.S, Sindarsingh Jebaseelan S.D "Hybrid Genetic Algorithm Assisted Artificial Bee Colony Approach for Voltage Stability Improvement" International Journal of Applied Engineering Research ISSN No.0973-4562 Research India Publications, Volume 10, Number 59 (2015) pp.534-541
10. S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.
11. X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," in IEEE Access, vol. 8, pp. 9260-9270, 2020, doi: 10.1109/ACCESS.2019.2963329.
12. D. Chang, S. Garg, M. Hasan and S. Mishra, "Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3152-3167, 2020, doi: 10.1109/TIFS.2020.2983250.
13. F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband and E. Salwana, "PSDS– Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud," in IEEE Access, vol. 8, pp. 118285-118298, 2020, doi: 10.1109/ACCESS.2020.3004433.
14. J. Zheng and L. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map," in IET Image Processing, vol. 14, no. 11, pp. 2310-2320, 18 9 2020, doi: 10.1049/iet-ipr.2019.1340.
15. Y. Zhang and B. Li, "The Memorable Image Encryption Algorithm Based on Neuron-Like Scheme," in IEEE Access, vol. 8, pp. 114807-114821, 2020, doi: 10.1109/ACCESS.2020.3004379.
16. H. Hu, C. Lin, C. Chang and L. Chen, "Enhanced secure data backup scheme using multifactor authentication," in IET Information Security, vol. 13, no. 6, pp. 649-658, 11 2019, doi: 10.1049/iet-ifs.2018.5380.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

17. Y. Song, Z. Zhu, W. Zhang, H. Yu and Y. Zhao, "Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture," in IEEE Access, vol. 7, pp. 84386- 84400, 2019, doi: 10.1109/ACCESS.2019.2923018.
18. W. I. Khedr, H. M. Khater and E. R. Mohamed, "Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage," in IEEE Access, vol. 7, pp. 65635- 65651, 2019, doi: 10.1109/ACCESS.2019.2917628.
19. W. Feng, Y. He, H. Li and C. Li, "A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm," in IEEE Access, vol. 7, pp. 181589-181609, 2019, doi: 10.1109/ACCESS.2019.2959137
20. H. T. Poon and A. Miri, "Fast Phrase Search for Encrypted Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 7, no. 4, pp. 1002-1012, 1 Oct.-Dec. 2019, doi: 10.1109/TCC.2017.2709316.
21. H. Lin, "Traceable Anonymous Authentication and Key Exchange Protocol for PrivacyAware Cloud Environments," in IEEE Systems Journal, vol. 13, no. 2, pp. 1608-1617, June 2019, doi: 10.1109/JSYST.2018.2828022.
22. A.A. Pammu, W. Ho, N. K. Z. Lwin, K. Chong and B. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1023-1036, April 2019, doi: 10.1109/TIFS.2018.2869344.
23. W. Luo, Y. Hu, H. Jiang and J. Wang, "Authentication by Encrypted Negative Password," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 114-128, Jan. 2019, doi: 10.1109/TIFS.2018.2844854.
24. C. J. Mitchell, "On the Security of 2-Key Triple DES," in IEEE Transactions on Information Theory, vol. 62, no. 11, pp. 6260-6267, Nov. 2016, doi: 10.1109/TIT.2016.2611003.
25. F. Guo, W. Susilo and Y. Mu, "Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 247-257, Feb. 2016, doi: 10.1109/TIFS.2015.2489179.
26. D. Godwin Immanuel and C. Chritober Asir Rajan, "An Genetic Algorithm approach for reactive power control problem," 2013 International Conference on Circuits, Power and

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 01, 2022

Computing Technologies (ICCPCT), Nagercoil, 2013, pp. 74-78, doi: 10.1109/ICCPCT.2013.6528940.