European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 10, 2020

Robust Retina Biometric Enhanced Paillier Cryptosystem for Privacy Preserving of Medical Data Stored in Cloud Environment

[1]MR.SREEHARI KUNDELLA, [2]DR. R.GOBINATH
[1]Research Scholar, Department of Computer Science, VISTAS, Chennai, Tamilnadu
[2]Associate Professor, Department of Computer Science, VISTAS, Chennai, Tamilnadu
[1]Kundella.sreehari@gmail.com, [2]drgobinathramar.scs@velsuniv.ac.in
Corresponding Author Email: Kundella.sreehari@gmail.com

ABSTRACT
In recent years the usage of cloud storage is increased tremendously and it influences effective maintenance of big data with low cost. As the cloud provides open services there is a highest chance of security breaches. There are several security schemes are in existence to protect confidential information stored in cloud. But still there is a lack in preventing information integrity and intruders can break the security by tampering keys involved in encryption and decryption while using standard cryptographic algorithms. This paper mainly focuses on the data integrity and confidentiality of the ECG big data stored in Cloud. The proposed model Biometric enhanced Paillier Crypto System (BPCS) comprised of three different stages. Initially, the retina of the data owner is acquired, preprocessed using the fuzzy dynamic histogram equalization and its significant features are extracted using SIFT variance. These extracted features of retina are used by paillier cryptography to generate the public key and private key, instead of using random numbers. The encrypted file is then converted to digital signature using ElGamalAlgorithm. The ECG encrypted file along with digital signature is uploaded in the cloud. If the cloud users need to access the file, then they have to use the public key of the data owner and using user's private key. They can verify the integrity of the file content by checking the hashing value. The simulation results evidenced the robustness of the BPCS by accomplishing security on cloud storage data more effectively and strongly while comparing with the standard security schemes.
Keywords: Big data, Cloud storage, biometric security scheme, paillier crypto system, retina feature extraction, digital signature, ElGamal algorithm

I. INTRODUCTION

Though, cloud offer a multitude advantageover big data and large opportunities, it carries baggages related to security issues which has to be mainly focused. The security issue often arises when the cloud user interacts through interfaces or applications, it mainly relies on Application Programming Interfaces (APIs) overall security [1]. While APIs are not protected properly then the hackers can easily enter inside the cloud and perform malicious actions. To overcome this problem, it is necessary to avail strong security authentication. Even though, the cloud service providers offersecurity schemes the access levels of users, guest and admin using the loop holes they may gain the advantage of the network and tries to perform malicious attacks.

Thus, cloud computing often faces many security challenges which includes various technologies like databases, networks, virtualization, operating system, management of transaction and memory, scheduling resources and concurrency control [2]. Most of these security challenges are applicable to cloud computing like the network which interconnects the cloud systems has to be secured. This paper concentrates on the data security which involves in data encryption along with ensuring the policies enforced during data sharing. There is a higher chance of malicious users pierce inside the cloud as a genuine user and breaks the confidentiality of the entire cloud. This will affect the secret information about the cloud consumers. The cloud suffers from four main security issues they are data, privacy, virus infected applications and security issues.

In general, the cloud consumers will always maintain their confidential data more securely by applying various authentication process for login interface instead of using password, the advanced models use behavioral and physiological biometric qualities such as face, fingerprint, ear, signature, palmprint etc. [3].

At the same time, the confidential files or information's of the data owners are not stored in cloud as such instead of that some cryptographic mechanism is applied to provide more security over confidential information's which are save on the cloud storage [4]. Before uploading the file to the cloud, it is encrypted using cryptographic algorithms and the crypted files are stored. When it has to be accessed, it is downloaded as the crypted file using the decryption process the original file content will be accessed by the authorized cloud consumers. Here, biometric cryptographic keys play essential role in encryption-oriented security in cloud computing paradigm.

Biometric based cryptosystem often unique and it authenticates based on their registered biometric traits. This paper provides the security to the big data of ECG Signals by adapting the concept of homomorphic encryption scheme. In this retina of cloud data owner is used as biometric characteristics and their features are extracted and using it two keys are generated they are public and secret keys. The public key is used to encrypt the content of the confidential file, here it is ECG dataset and the encrypted file alone is stored in the cloud. Even if the intruders get the control to access the file, it will be only in the encrypted format. When the legitimate user needs to access the encrypted file, they have to use the secret key to decrypt it. Thus, whenever a user tries to read the file, it is only decrypted using that key used to encrypt in homomorphic encryption. Additionally, the non-repudiation is also considered as important factor in this work by applying digital signature the authenticity of the big data will never be comprised in cloud environment.

II. RELATED WORKS

Sasidhar et al. [5] in their work investigated and reported that multimodal biometric scheme which offers increased significant performance compared to unimodal for high volume of data.

Anwar et al. [6] stated that using more biometric integrated security scheme like finger stripe and hand geometry it produces high recognition rate compared to single biometric based security scheme. Mishra et al. [7] in their work examined different kinds of multimodal biometric with different fusion methods based on their suitability and advantage of using multiple biometric traits and produce best result compared to conventional single biometric system.

Alvarez et al. [8] devised template of iris biometric based method which produce higher security level by adopting fuzzy extractors. Using biometric trait, the security value is obtained to ensure authentication of confidential data. Popovic et al. [9] explains cloud computing security

problems, in their study they determined remote resource location and virtualization method leads to more vulnerable attacks in cloud environment. They also discussed about information integrity as an essential factor for security.

Mathisen et al. [10]defines in their work various schemes of security issues in cloud computing. If the service providers of cloud don't follow strict security schemes then it will consequence to vulnerable attacks. Duarte et al. [11] analyzed security and privacy of data maintained in cloud environment. They stated that thrust worthiness is an important factor to acquire confidence among cloud users. Vishruti et al. [12] proposed biometric authentication-based security scheme for securing images using cryptography algorithms. In this work two major process are done they are image compression and encryption by applying discrete wavelet transform and SHA with blowfish algorithm respectively. Masala et al. [13] in their work constructed open stack model by exploring multimodal biometric security approach. This work ensures high level of protection of data stored on cloud servers. It also performs data fragmentation to achieve protection at high level.

III. METHODOLOGY: RETINA BIOMETRIC ENHANCED PAILLIER CRYPTOSYSTEM WITH INFORMATION INTEGRITY OF BIG DATA CLOUD STORAGE

The complete structure of the proposed retina biometric enhanced paillier cryptosystem for cloud data protection is illustrated in the figure 1. Initially, before uploading the ECG file of the patients on the cloud it is encrypted using paillier cryptosystem, where its public key and private key are generated by the features extracted from the retina of the data owner. The encrypted files integrity is preserved by applying hashing function to generate the message digest and which in turn is encrypted by the Elgamal algorithm to generate the digital signature. Finally, along with the encrypted file the digital signature is attached and uploaded in the cloud. The cloud users who needs to access the file has to decrypt the file using the owner public key and the message digest is obtained on the decrypted plaint text and the digital signatures are compared to verify its integrity, genuineness and confidentiality of the proposed BPCS security scheme.

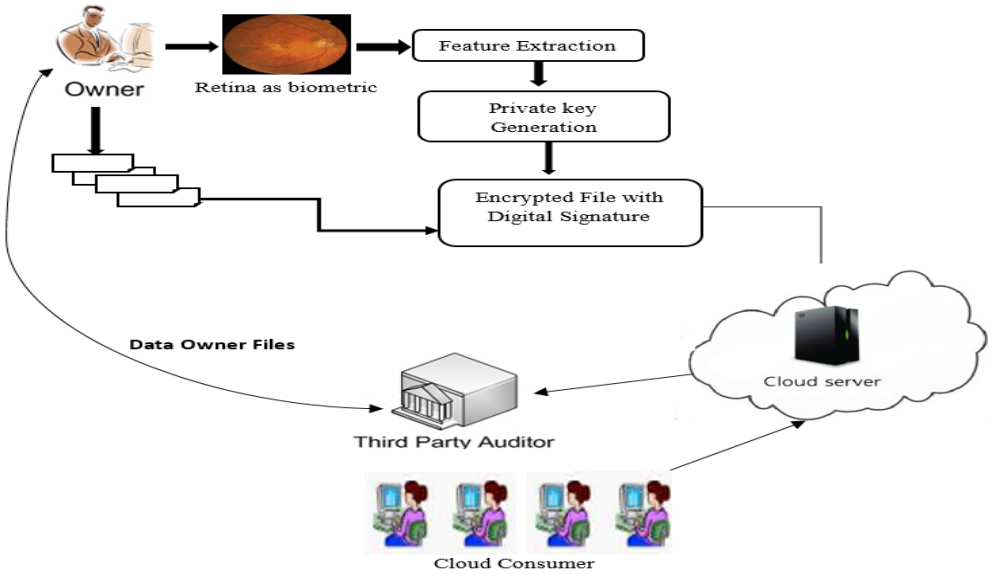

Figure1: Overview of proposed Biometric Paillier Cryptosystem based Secured ECG File storage in cloud paradigm

A. Retina Feature Extraction

It is very difficult to perform preprocessing on retinal images because of its intrinsic characteristics. In presence of noise retinal images suffers with poor and different contrasts which occurred due to camera flash reflection and pigmentation of retina. When the illumination is uneven it results in intensity level increase near Optic Disc (OD) and decreases intensity level in faraway regions. To distribute intensity of retina image it is essential to find the histogram which denotes number of pixels for each level of intensity. When there are more pixels for certain intensity the peak exposes its higher level.

B. Histogram Equalization of Retinal Image

To improve contrast in retinal images, histogram equalization is applied to accomplish effective spreading of most frequent intensity values [14]. This is achieved by increasing global contrast of retina when its data is very essential. A color histogram represents number of pixels belonging to different types of color components. In this case histogram can't be applied directly to RGB components so that it has to be converted to either HSV or HSL, then algorithm can be applied to luminance channel without disturbing hue and saturation of retina image [15].Hence Histogram Equalization is very essential on considering these factors which produce significant effect and, in this work, Dynamic fuzzy color intensity histogram equalization is developed.

C. Computation of Fuzzy Histogram

Fuzzy histogram is a series of real number hst(i), i ∈{0,1, …, LV -1} where hst(i) refers to the occurrence of gray levels frequency that are near to i. The gray value ISY(x,y) of retinal image is represented as $\widetilde{ISY}$(x,y), then membership value for each pixel $\mu_{ISY(x,y)i}$and fuzzy histogram is calculated as follows

$$\mu_{ISY(x,y)i} = maximum\langle 0,1 - \frac{|ISY(x,y) - i|}{4}\rangle$$

$$fzh(i) \leftarrow fzh(i) + \sum_x \sum_y \mu_{ISY(x,y)i}, M \in [a,b]$$

In this retina preprocessing, the inexactness of gray value is handled better by applying fuzzy statistics while comparing with classical crisp histogram methods. Thus, the fuzzy histogram is much suitable for this retinal feature extraction.

D. Histogram Partitioning

In this process multiple sub histogram are partitioned based on the local optima. Each valley area among two consecutive local maxima frames a partition. The peaks of the histogram won't be remapped while performing dynamic equalization on those sub histograms. This process will preserve the mean image brightness more effectively. Using fuzzy histogram's first and second derivate local maxima are located. Central variance operator is used for handling discrete sequence of data and it is computed as

$$\dot{hst}(i) = \frac{dfhst(i)}{di} \triangleq \frac{hst(i+1) - hst(i-1)}{2}$$

Where, hst(i) refers to fuzzy histogram of ith intensity level and $\dot{hst}(i)$denotes its first order derivative. Second order central variance operator is used for second order derived which is directly applied on fuzzy histogram. This will reduce the error rate occurred during first order derivate

$$\ddot{hst}(\iota) = \frac{df^2hst(i)}{dfi^2}\Delta hst(i+1) - 2hst(i) + hst(i-1)$$

Where $\ddot{hst}(\iota)$ signifies the fuzzy histogram's second order derivative of ith intensity level. The local optima points are shown for the level of intensity values in which first order derivativeswith second order negative value is also determined using the equation

$$i_{max} = i\forall\{hst(i+1) \times hst(i-1) < 0, hst(i) < 0\}$$

When the zero crossing was not occurred at perfect integral values the ambiguity arises, to overcome that highest count of point is persevered among as maxima among neighboring pairs.

The partitions are formed using local maxima points presented in fuzzy histogram of retina image. The local maxima detected is signified as $\{lm_{0,}lm_{1,}, \dots, lm_{n,}\}$ are involved in partitions. Let us consider that fuzzy histogram range is spread with in the range of$[ISY_{min}, ISY_{max}]$. The sub-histogram attained after the partitioning of sub histograms are defined as

$$\{[ISY_{min}, lm_0], [lm_0 + 1, lm_1], \dots, [lm_n + 1, ISM_{max}]\}.$$

Each sub-histogram is equalized individually using two operations mapping partitions into dynamic range and applying histogram equalization by applying spanning function.

$$spn_i = hgh_i - lw_i$$

$$ftr_i = spn_i \times log_{10}TN_i$$

$$rng_i = \frac{(L-1) \times ftr_i}{\sum_{k=1}^{n+1} ftr_k}$$

Wherehgh_irefers to highest intensityvalue, lw_i is the lowest intensity value of i^{th}input sub-histogram, $TN_i$is thetotal pixels presented in that concern partition. The concern sub-histogram given as input is definedby spn_i, whereas$range_i$ refers to dynamic range used in the output sub-histogram. rng_iSignifies the ith sub-histogram outputs dynamic range which is formulated as

$$srt_i = \sum_{k=1}^{i-1} rng_k + 1$$

$$stp_i = \sum_{k=1}^{i} rng_k$$

Between two extremities, the exceptions are presented

$$[srt_1, stp_1] = [0, rng_1] and [srt_{n+1}, stp_{n+1}] = \left[\sum_{k=1}^{n+1} rng_1, L-1\right]$$

Sub-Histogram Equalization

Each partition of the histogram is equalized using global histogram histograms equalization as it is remapped in the following equation

$$NY(j) = srt_i + rng_i \sum_{k=start_i}^{j} \frac{hst(k)}{TPM_i}$$

Where NY(j) is the new intensity level related to the jth intensity level on the retina image, hst(k) is the kth intensity level histogram value on fuzzy histogram and $TPM_i = \sum_{k=srt_i}^{stpi} hst(k)$ denotes total population count in the ith histogram partition.

IV. FEATURE EXTRACTION OF RETINA USING SIFT ALGORITHM

In this work to extract the distinct invariant of retina image is achieved by applying scale invariant feature transformation (SIFT). SIFT algorithm is very robust to several changes like rotation, scaling, distorted, noisy and blurred. SIFT algorithm is applied to extract significant features of retina key points. This algorithm comprised of four major steps they are space to space detection, key point localization, assignment of orientation and descriptor of key point [16]. The potential points of retinal image are determined by Difference of Gaussian Function (DOG). This algorithm is a feature extraction that subtracts one Gaussian blurred original image with less blurred of another image.

$$DG(y, z, \sigma) = SG(y, z, k\sigma) - SG(y, z, \sigma) * Inp(y,z)$$
$$= LC(y, z, k\sigma) - LC(y, z, \sigma)$$

Where SG (y, z, σ) refers to variable scale Gaussian, * denotes the convolution operator, Inp(y, z) is the input retinal image, DG (y, z, σ) is the Difference of Gaussian with k scale time. During key point localization both low contrast points and edge response are eliminated. Principal curvatures are calculated using hessian matrix and the key point which have a ration among principal curvatures greater than the ratio are eliminated. Sample points are used to form gradient orientations within a region near the key-pints to obtain orientation assignment. The feature extraction is shown in the figure 2.

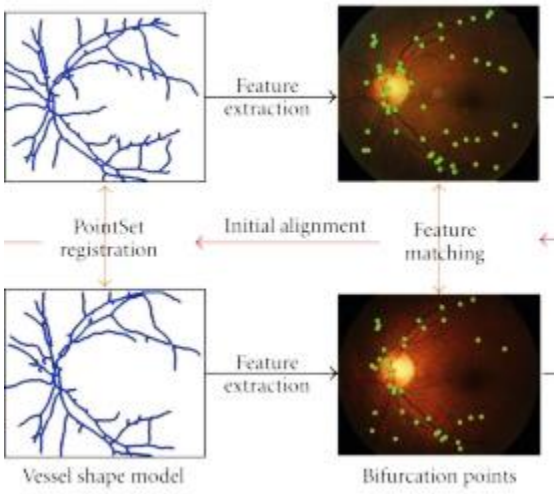

Figure 2:Retinal Feature Extraction

A. Paillier Cryptosystem

In this paper homomorphic cryptosystemknown as Paillier Cryptosystem [17] is applied to secure the ECG dataset while storing in cloud. Contrast to standard cryptography, the paillier cryptography use additive homomorphism [18] in this message can be added along with encrypted code and at the same time decryption is done perfectly. This paillier crypto has its own unique characteristics and extension of public key cryptography with modular functionality. In this work ECG file is encrypted using paillier cryptography. It has three main stages they are public-private key pair generation, ECG file Encryption and ECG file Decryption.

Key Generation

In paillier cryptanalysis two prime numbers t and v. The values of c and d are multiplied and stored as m. An integer value which is non-zero with semi arbitrary value g has to be selected with the criteria that W*n2 measured in terms of invertible units. In this proposed work the key generation of Paillier public key encryption is done by extracting the retina features in a random manner as security parameter Irk as input and it generates a two big prime numbers c and d, m = cd and μ = lcm(c-1, d-1). The method chooses arbitrarily $h \in Y^*_{m^2}$, in such a way m divides the order of h. It can be guaranteed by inspecting gcd(c*d, (c-1)*(d-1)) = 1. The pair (m, h) is the public key and private key is μ.

ECG File Encryption

File encryption works on message msg within the range of 0 to m. select the arbitrary number rnd whose range lies between 0 and m. The original file is converted to cipher text by computing

$$CT = h^{msg}. rnd^{m}. m^2$$

ECG File Decryption

Once the receiver receives the encrypted file, they perform decryption process by applying the formula

$$PT = L(CT^{\mu} \bmod m^2)\ \beta \bmod m$$

Where CT values is between 1 and m^2

B. ElgamalDigital Signature

Digital Signature is utilized in this proposed work to enable the information integrity in order to ensure that the message passed to the receiver is not alter and to authenticate that the message is created by the data owner (sender) and thus non-repudiation cannot be done by the sender. Here, the file which before loaded to the cloud, it under goes hashing, in which hashing algorithmperforms message digest operation, where the file is crunched to a short line known as message digest. The message digest is now encryption using the Elgamal algorithm [19] to form the digital signature.

Steps involved in Digital signature process: Using MD5 algorithm Message Digest is created for the ECG File before loading it to the cloud.The message digest is encrypted with the private key generated by retina feature using ElGamal Algorithm known as digital signature.Public key of signer is used for verification of the message authenticity. Both the figure 3 and 4 shows the Retina based Cloud security using Enhanced Paillier Crypto system.

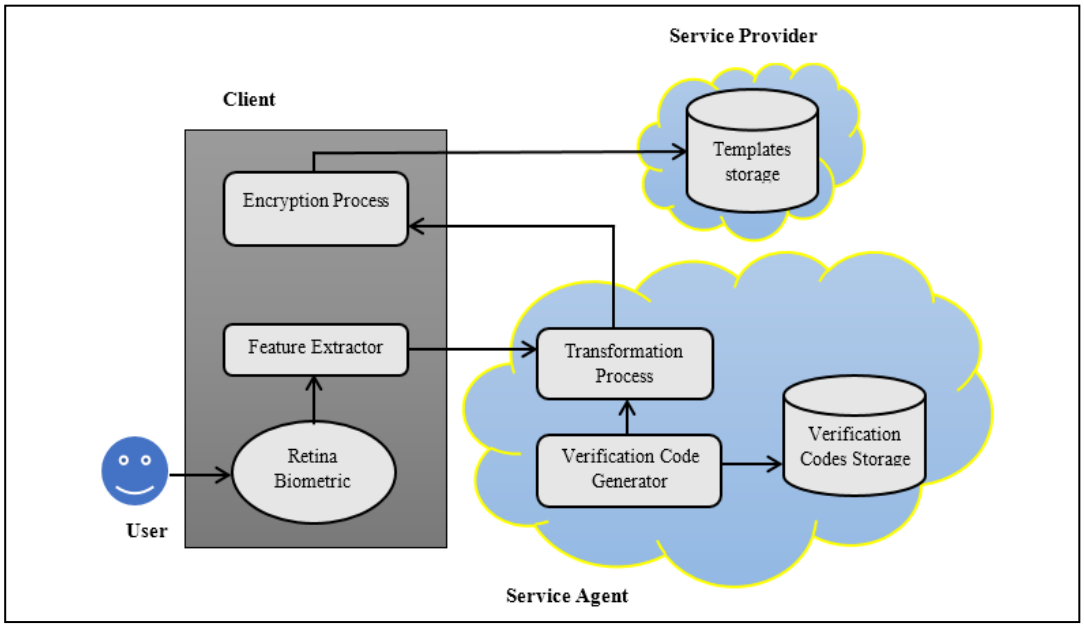

Figure 3:Process of Enrolling Retina Biometric based Cloud security

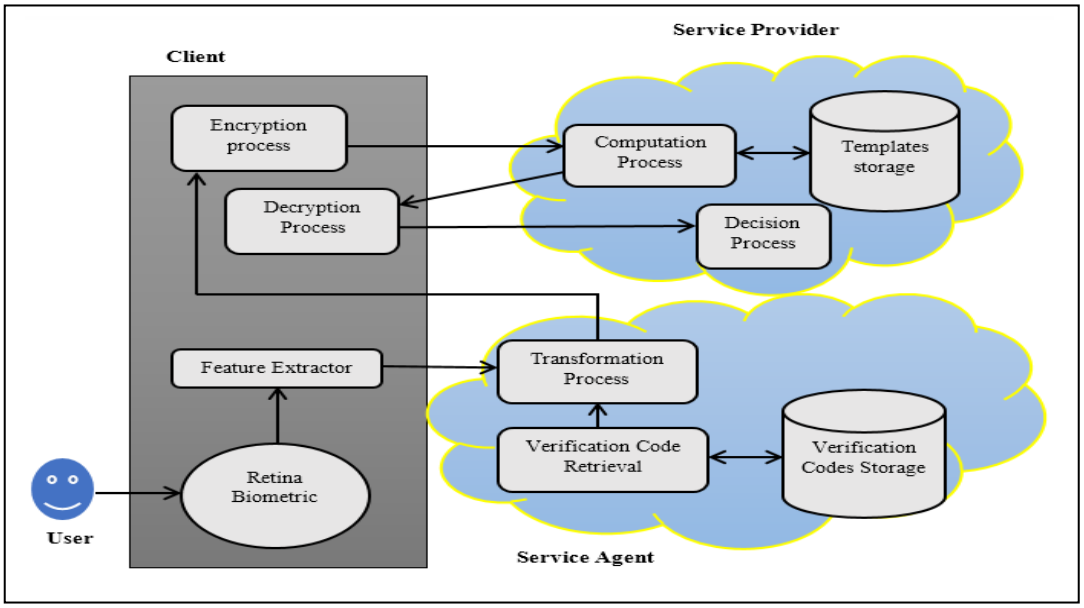

Figure 4:Verification of Cloud owner and File Confidentiality

Algorithm: Retina Biometric based Paillier Cryptosystem with Enhanced Information Integrity of ECG Files stored in Cloud

Input: Retina image, ECG Files
Output: Encrypted File, Digital Signature
Procedure
Begin
Stage 1: Retina Image Feature Extraction

1.1 Acquire the retina image from the data owner
1.2 Perform preprocessing to enhance the retina image using Fuzzy Dynamic Histogram Equalization
1.3 SIFT Variance is applied on retina image to extract the significant features

Stage 2: Paillier Crypto System – Key Generation

2.1 Choose two large prime number c and d from the security parameter Ir^k as input and with the condition gcd(c*d, (c-1)*(d-1)) = 1. The both prime numbers are in equal length.
2.2 Compute m = c*d and μ = lcm[(c-1, d-1)]
2.3 Select random integer h, where $h \in Y^*_{m^2}$
2.4 Check m separates the way of h by investigativeexistence of the ensuing modular multiplicative inverse $\beta = (L(h^{\mu} \bmod m^2))^{-1} \bmod m$, whose function M is well-defined as $L(y) = \frac{y-1}{m}$
2.5 The Public key used for encryption is denoted as (m,h).
2.6 The Private key involved in decryption is represented as μ

Encryption of ECG File

2.7 Let E be anECG data to be encrypted where 0≤msg≤m.
2.8 Select random value rnd which is indicated as 0≤rnd≤n with the condition gcd(c*d, (c-1)*(d-1)) = 1
2.9 Compute ciphertext$CT = h^{msg}. rnd^m. m^2$

Decryption of ECG File

2.10 ConsiderCT be ciphertext to decrypt, where $CT \in Y^*_{m^2}$.
2.11 Compute plain text message PT using the formula

$$PT = L(CT^{\mu} \bmod m^2)\ \beta \bmod m$$

Stage 3: Elgamal Digital Signature Generation

3.1 The Message PT is signed as

- Choose a prime number prm and select an integer k from {2,.. prm-1}
- Calculate $t = h^k \bmod prm-1$
- Calculate v = (Hash(PT) -xt) k mod (prm-1)
- Signature generated is (t,v)

3.2 Verification Process

- Verify 0 < t <prm and 0 < v < prm-1
- Signature is validated only if $h^{Hash(PT)} \equiv y^t t^v \pmod{prm}$

End

V. RESULTS AND DISCUSSIONS

This section discusses about analyzing the performance of the proposed Biometric based Paillier Crypto System (BPCS) for protecting the ECG Data stored in Cloud Storage. The proposed model BPCS is implemented using python code and its performance is evaluated with other security schemes namely RSA Algorithm, Standard Paillier Cryptography (PCS). The evaluation metrics used in this work are False Match Rate, False Non-Match Rate and Accuracy.

A. Performance Analysis based on False Match Rate (FMR)

False Matching Rate (FMR) is the possibility that the machine incorrectly suits the enter pattern to a non-matching template within the database. It measures the percent of invalid inputs that are incorrectly generic. In case of similarity scale, if the man or woman is an imposter in fact, but the matching rating is better than the brink, then he is treated as true. This will increase the FMR, which thus also relies upon the edge rate. False Match Rate (FMR) is calculated by finding the number of authenticated users that are mistakenly identified as genuine users. The percentage of the impostor tries that are incorrectly stated to match a pattern of another user. The FMR is formulated as follows:

FMR = No. of. False Positives / (No. of. False Positive + No. of True Negative)

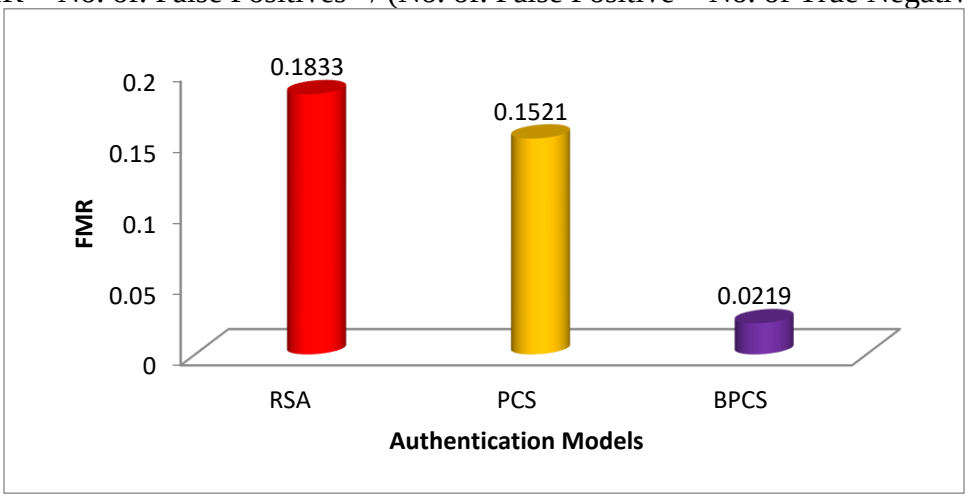

Figure 5: Performance Analysis based on False Matching Rate

From the figure 5shows the performance of the three different authentication models used for protecting ECG Big data in Cloud based on their False Matching Rate. The proposed model Biometric enhanced Paillier Crypto system (BPCS) produce less false matching rate compared to other RSA and Paillier Crypto System. Because security mechanism provided by the BPCS is very strong as it integrates the iris biometric to generate the private and public keys of paillier crypto system. The data integrity is also maintained by BPCS to achieve the authenticity of the ECG data file stored in the cloud. BPCS produce less false matching rate 0.0219 while RSA and PCS produce 0.1833 and 0.1521 respectively. BPCS produced less FMR, but the security point of view it is very strong compared to other RSA and Paillier Crypto System.

B. Performance Analysis based on False Non-Matching Rate(FNMR)

False Non-Matching Rate (FNMR) is the opportunity that the machine fails to detect a in shape between the enter pattern and a matching template within the database. It measures the percentage of legitimate inputs which are incorrectly rejected.The False Non-Matching Rate

(FNMR) is calculated by finding ratio of genuine attempts that are incorrectly not to match a pattern of the same user. Determining two retinal biometric are not from same identity, but in real they are actually is known as False Non-Matching Rate.

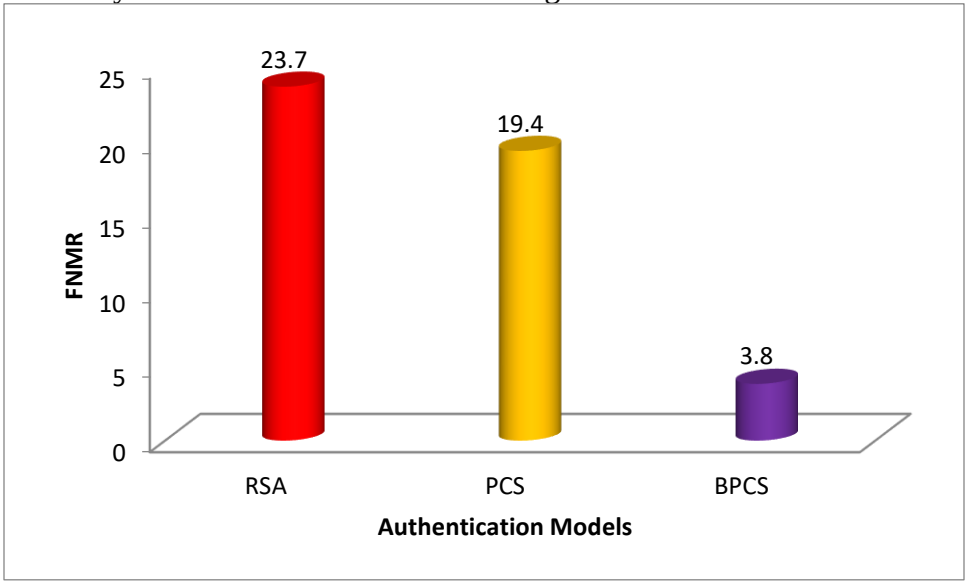

Figure 6: Performance comparison based on False Non-Match Rate (FNMR)

The performance analysis based on False Non-Matching Rate (FNMR) produced by three different authentication models such as RSA, PCS and BPCS is shown in the figure 6. The result explores that the FNMR produced by proposed BPCS is very less compared to RSA and PCS. This is because of the BPCS uses retinal image of the data owner to generate keys for paillier cryptography to encrypt and decrypt the ECG files. The data integrity of the confidential file is strengthened by applying Elgamal digital Signature algorithm. The genuine user is maximum detected by the proposed BPCS model thus it produced less FNMR with the rate of 3.8%, RSA and Paillier cryptography algorithms uses the random values to generate the private key and public key and they produced 23.7% and 19.4% respectively. BPCS produced less FNMR, but the security point of view it is very strong compared to other RSA and Paillier Crypto System.

C. Performance Comparison based on Accuracy of Security Schemes

Accuracy is defined as the total number of genuine and imposter user's access correctly detected by the security schemes to the actual number genuine and imposter access done to access the ECG file in the cloud.

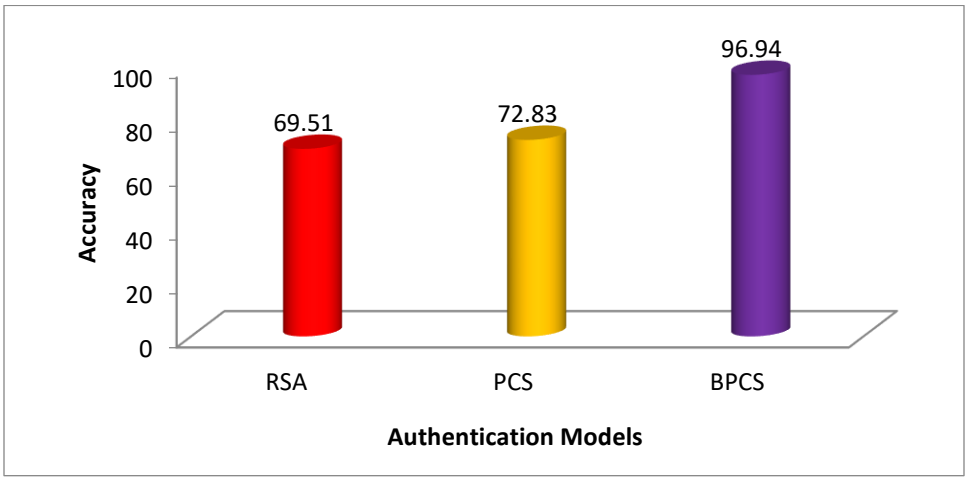

Figure 7: Comparative Analysis of Accuracy of Authentication Models

The accuracy of the security scheme applied on cloud storage to maintain ECG big using three different authentication models is depicted in the figure 7. The BPCS produced highest accuracy in determining and authenticating the genuine cloud users by applying retina biometric enabled paillier cryptography with assurance of data integrity achieved using Elgamal digital signature. The avoidance of non-repudiation and confirming confidentiality of the ECG file stored in Cloud storage are the biggest merit of the BPCS to achieve the accuracy rate of 96.94%, while comparing with RSA 69.5% and PCS 72.83%. BPCS has provided highest accuracy compared with other models such as RSA and PCS.

VI. CONCLUSION

This work focuses on accomplishing high security to the ECG big data stored in cloud computing. As the security scheme is one of the vital objectives of the big data this is achieved in this paper by constructing a robust and powerful crypto system known as retina biometric enabled Paillier crypto system which guarantees the data integrity. Retina is preprocessed and its contrast is enhanced using fuzzy dynamic histogram equalization and its extracted feature is used for biometric key generation.Security scheme of the proposed BPCS provides strong security to ECG files using paillier crypto system which uses retina biometric features as keys for encryption and decryption. The information integrity is verified is done by generating the digital signature using ElGamal algorithm which greatly helps during verification of authenticity of the file content and accountability of the cloud owner.In this paper the performance ECG data has been analyzed with three authentication models such as RSA, PCS and BPCS.

The proposed BPCS authentication model has produced lessFalse Matching Rate of 0.0219% and False Non-Matching Rate of 3.8% respectively compared toother authentication models such as RSA and PCS. But the security point of view BPCS is very strong.The simulation results proved the robustness of the proposed BPCS provides prominent security to the cloud data comparing to the standard RSA and Paillier Cryptography. BPCS produced high accuracy of 96.94% for secured access and less mismatching error rate, hence it is more effective in providing cloud storage security compared to other two models such as RSA and PCS. Thefuture work is to use, secured secret sharing algorithm to optimize the cloud data security. The future

work is to use secured secret sharing algorithm tooptimize the cloud data security and It develops MapReduce based security mechanism to improve thebig data security in cloud computing.

REFERENCES

1. Panteli N, Dawson, P. Video conferencing meetings: Changing patterns of business communication, New Technol. Work Employ. 2010, 16, 88–99.
2. H. Takabi, J.B.D. Joshi and G.-J. Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8(6), 2010, pp. 24-31.
3. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2740–2749.
4. S. Kavin Hari Hara Sudhan, S. Saravana Kumar "An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme" Indian journal of science and technology Vol 8, No. 35, December 2015.
5. Sasidhar K, Kakulapati VL, Ramakrishna K, Kailasa-Rao K. Multimodal biometric systems-study to improve accuracy and performance. Int J Compute SciEng Survey 2010; 1: 54-61.
6. Anwar F, Rahman MA, Azad S. Multi biometric systems-based verification technique. Euro J Sci Res 2009; 34: 260-270.
7. Mishra A. Multimodal biometrics it is: need for future systems. Int J ComputAppl 2010; 3: 28-33.
8. Hernández Alvarez F, Hernández Encinas L, Sánchez Ávila C. Biometric fuzzy extractor scheme for iris templates. Proceedings of World Congress in Computer Science, Computer Engineering, and Applied Computing, WORLDCOMP, 2009.
9. Mathisen E (2011) Security Challenges and Solutions in Cloud Computing, Vol. 5
10. Popovi´c K, Hocenski Z (2010) Cloud computing security issues and challenges, Vol. 2010. Opatija, Croatia
11. DuarteT, Piementao JP, Sousa P,Onofre S (2016) Biometric access controlsystems: a review on technologies to improve their efficiency.In: Power Electronics and Motion Control Conference (PEMC),IEEE, pp 795–800
12. VishrutiKakkad,Meshwa Patel, Manan Shah, Biometric authentication and image encryption for image security in cloud framework Multiscale and Multidisciplinary Modeling, Experiments and Design, 2019-12
13. Masala, Giovanni &Ruiu, Pietro & Grosso, Enrico. (2018). Biometric Authentication and Data Security in Cloud Computing. 10.1007/978-3-319-58424-9_19.
14. K. Hasikin and N. A. M. Isa, "Adaptive fuzzy contrast factorenhancement technique for low contrast and non-uniformillumination images," Signal, Image and Video Processing, 2012.
15. M. M. Fraz, W. Jahangir, S. Zahid, M. M. Hamayun,S. A.Barman, Multiscale segmentation of exudates in retinal imagesusing contextual cues and ensemble classification, BiomedicalSignal Processing and Control, vol. 35, pp. 50–62, 2017.
16. Lowe, David G. (2004). "Distinctive Image Features from Scale-Invariant Keypoints". International Journal of Computer Vision. 60 (2): 91–110.
17. Kocabas O, Soyata T. Medical data analytics in the cloudusing homomorphic encryption. In Chelliah PR, Deka G(eds.): Handbook of Research on Cloud Infrastructures forBig Data Analytics. Hershey, PA, USA: IGI Global, 2014,pp. 471–488.

18. Paillier,Pascal."Public-KeyCryptosystemsBasedonCompositeDegreeResiduosityClasses."Advances inCryptology–EUROCRYPT '99 1592 (1999):223-238. 15 Apr.2008.
19. TaherElGamal (1985), A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory. 31 (4): 469–472
20. Rivest RL, Shamir A, Adleman L. A method forobtaining digital signatures and public-key cryptosystems.ACM, 1978;21(2):120–126
21. Arunachalam, A. S., and A. P. Hidhaya. "Locating nearest neighbor using privacy query based on improvised paillier cryptosystem." Journal of Advanced Research in Dynamical and Control Systems Vol.5 pp: 176-182, 2017.
22. Ms V. Divya, Dr. R. Gobinath ," Routing Protocol And Security Threats In Manet", International Journal Of Scientific & Technology Research Volume 9, Issue 04, Pp: 799-802, April 2020