Enhanced Framework for Ensuring Privacy Preserving Image Retrieval in Cloud

Jitendra Kumar Gothwal, Kunam Subba Reddy

Abstract*: Large scale of images data sets are being produced every day by various digital devices. Due to huge computational jobs make people seizure to cloud platforms for their efficient & economical reckoning resources. These computing platforms in which assets are provided as services of the internet. Sensitive information stored in cloud makes more challenging in data security and access control. Once data is uploaded to cloud-platform, the privacy and security of image-data fully depend and believe upon cloud service provider honesty. Our proposed work deals with securing image where high protections are applied on multimedia contents. This paper deals with studies security challenges algorithms lies in image at the time of constructing cloud platform. In this a new enhanced security technique investigated, includes secure by using computation and encryption, act as a security information guard for high secrecy in cloud platform data storage areas. In our research work, cipher-text image is created and performing encryption-decryption at User level. Data hiding and ECC (Elliptic curve cryptosystem) based watermarking technique at cloud computing platform.

***Keywords* : Cloud, internet, privacy and Security, encryption, decryption, elliptic curve cryptosystem, watermarking**

I. INTRODUCTION

Now in present days emerging technology development in Cloud computing includes sharing of computing resources and has many challenges in various aspects of image information handling. It stores and manages frequently used data on multi servers that could be accessed later by using the availability of Internet. The advantage of adopting cloud computing is it saves user from incurring the heavy cost of hardware and software services. Before emerging of cloud computing, users/companies faced problem- there are high chances that user may lose his image data or company data, if there is hardware or software failure.

There are several high securities regarding client's trust, leakage of data, user's authentication, data loss and some malevolent user handling in cloud platform. When wrong use of cloud computing and the services given then Hijacking of data, loss of control and some disturbance may be there in the cloud. Hence vital importance of improving the security and data storage in platform of cloud computing. There are several high securities regarding client's trust, leakage of data, user's authentication, data loss and some malevolent user handling in cloud platform.

It is very important and necessary for the data storage hub in cloud computing with high security solutions. So the entire storage of data in cloud computing platform is with full trustable and reliable. The security in the cloud computing storage hub should be flexible so as per required, improved by new security algorithm.

This research paper focuses on a solution to allow an concerned party to identify overall feature of image data with no conciliating user's data privacy. In this proposed research method, the concern interested parties carry out one of the image detection algorithms to produce the features of an image from the encrypted image-data which is shared by Network Service provider [1]. Service provider can utilize the comparisons and similarity between the features extracted in the user's image data and the standard specified images to identify end users. Against the interested party the privacy of user's image is challenge to preserve. While permitting the useful features of detection algorithm over encrypted image-data. To manipulate this challenge, we intend an enhanced security system on image-data which exploits Homomorphic encryption method to crumble the present-exist image-data feature detection algorithm that can be carried out in cipher-data-text domain.

II. CLOUD SERVICES AND MODELS

There are various services and models in cloud computing, which provides the cloud computing suitable and easily accessible to users. Cloud Computing provides four main deployment models as shown in figure-1and four basic service models. A cloud deployment model depends on "configuration" of cloud domain factors, which are: Public, Private, Hybrid, and Community and in cloud access belongs to any of one. The public cloud systems and services are mainly available to the general public and may be some possibility of less secure because of its directness. The Private cloud infrastructure allows systems and services provisioned for exclusive use within an organization and it provides high security, privacy and reliability because of its network environment. The community cloud infrastructure is provisioned to be accessible by a specified organizations group having shared concerns. Hybrid cloud infrastructure is the combination of a private and public cloud, with flexibility and control.

Revised Manuscript Received on October 05, 2019.

Jitendra Kumar Gothwal[1],Professor, Computer Science & Engineering Department, Rajeev Gandhi Memorial College of Engineering & Technology (Autonomous) , Andhra Pradesh, India.

Kunam Subba Reddy[2] Professor, Computer Science & Engineering Department, Rajeev Gandhi Memorial College of Engineering & Technology (Autonomous), Andhra Pradesh, India

On these platforms critical workloads or sensitive applications are carried out by using private cloud and while having the non-critical workloads or applications are carried out by using public cloud.

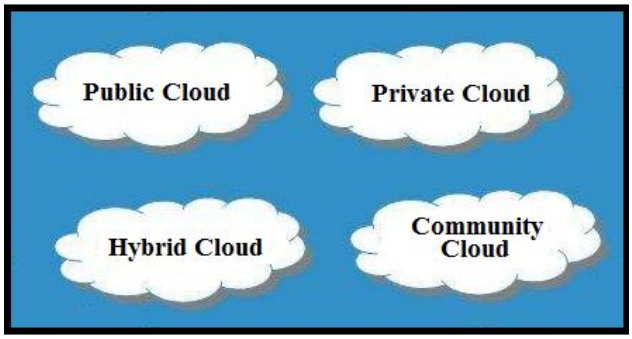

Fig. 1. Deployment Model

Cloud computing is collection of four service models and are categorized as: IaaS (Infrastructure as a service), Paas (Platform as a service), SaaS (Software as a service) and FaaS (Functions as a service) as shown in figure-2.These service models act as cloud computing stack ,because their structure build on top of one another [2].

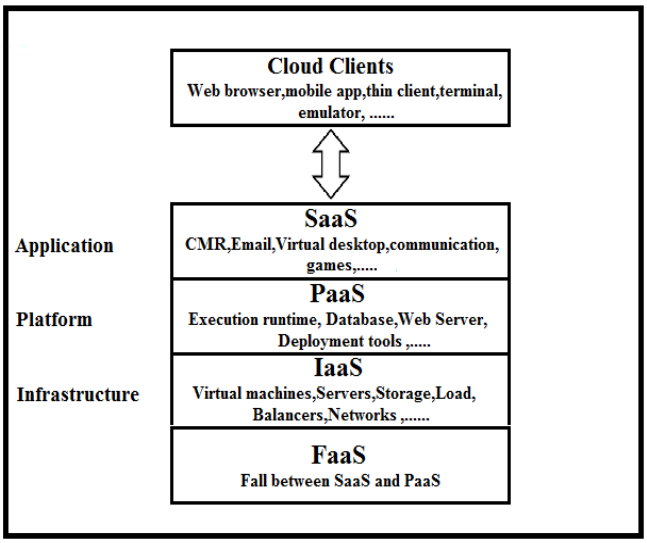

Fig. 2. Service model

IaaS is one of the most basic fundamental service models of cloud computing that allows IT infrastructure like virtual server space or VM's on rent from the service provider from cloud computing platform on pay-for-service center. PaaS (Platform-as-a-service) refers to deploy onto the cloud service infrastructure acquired applications for developing on-demand condition, delivering, managing and testing of software applications. In SaaS (Software-as-a-service) the cloud service provider leases applications or softwares, connected to the internet, as per the demand and on a subscription basis. These lease applications and softwares allow the cloud service provider to be control over investment for software design architecture; support operations; maintenance and client focus on the actual software and application being used. FaaS refers to cloud version of "serverless computing architecture", adds another layer of concept to PaaS, allows software development and free the user from managing, so that developers are completely insulated from everything and upload instantly functional blocks of code and set them to be triggered by a certain event.

III. IMAGE-DATA PROCESSING: PRIVACY PROTECTION

The proposed research system Architecture as shown in figure-3 consists of cloud server model and its architecture in public cloud. Here User holds huge image-data act as data-owner and proposes to frame-out the image-data processing jobs to the cloud computing platform. As per the System Architecture Model, User encrypts the image-data earlier in advance before carry-outing to the cloud computing platform, which is poised by different-set of cloud servers. It can accept responsibility to be Honesty-and-Trustful with snooping. Cloud Server Platform can only right to access the encrypted image-data which is uploaded by the User-owner and carry-out the relevant image processing algorithms over cipher-text data domain. Then the cloud server in cloud computing platform precedes the demanded results back in cipher-text form to the user. After this , in last, User use its private key and process to decrypt the data to get returned concern results. In this entire system, the cloud computing platform should not have any involvement to access the User results carried-out by image-data computation jobs in the domain of plaintext

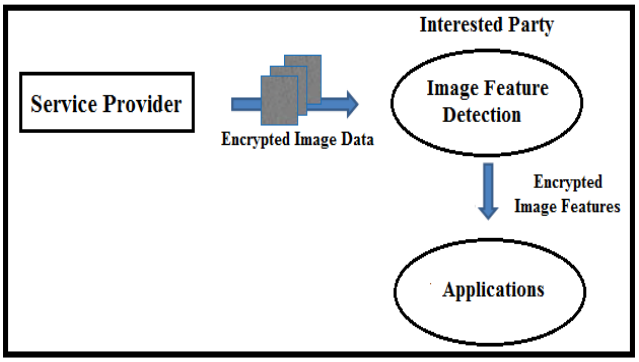

Fig. 3(a). Cloud System Model

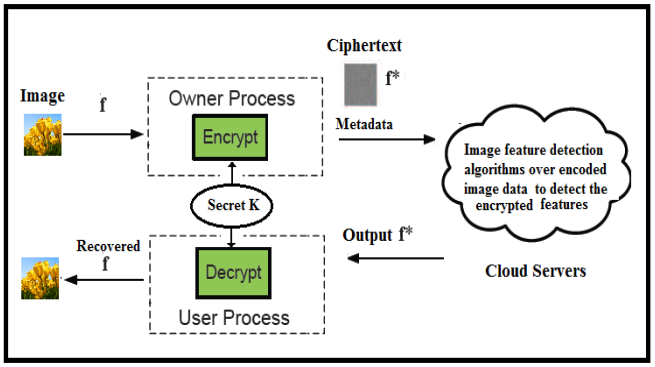

Fig. 3(b). Architecture in public Cloud [4]

IV. SYSTEM DESIGN

A. Image Data Preprocessing:

Now a day image-data processing applications are installed or set-upped in large variety of end-user devices and are widely used for data transfer. So it is essential and important to encrypt an image before sending to anyone as per security point.RGB pixel displacement is the best method to encrypt the color-data image. In this RGB

technique, shown in figure-4, input data is encrypted by using another color-data image which act or used as a Key-Image, and here important point is Key-Image is of equal and same size with the given color data-image i.e. original color image. Now the key generation process involves the splitting of taken Key-Image into Red, Green, Blue components and then bit plane of each Red, Green, Blue components is selected, which operates as a KEY. Then we also split the original color data-image into Red, XORed with the Key-Image components and by this operation transitional cipher-text Image will be generated. This further endures as shown in figure-5, scrambling of RGB and provides the required Cipher Image [5]. Here in this research, the original image is encrypted with the key image. Encrypted data image is accessible by one who is having the same Key-Image. When decryption of the Image is processed then it follows reverse process of encryption.

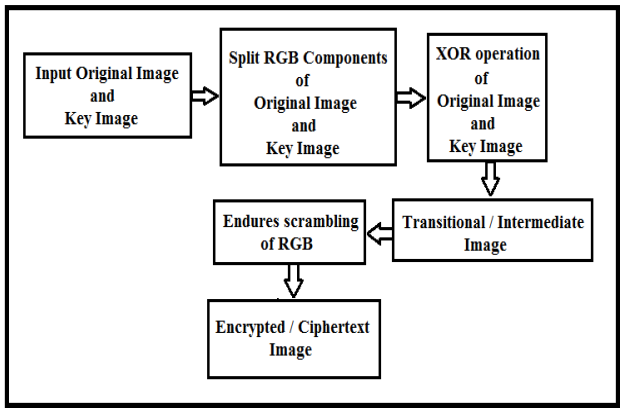

Fig. 4. RGB pixel displacement Encryption

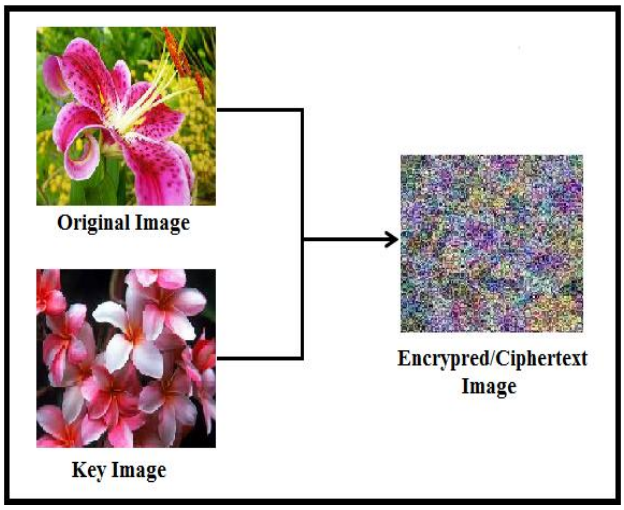

Fig. 5. Generation of Encrypted/Ciphertext Image

B. Privacy-Preserving Image Processing (Encrypted Image Evaluation):

In cloud computing platform to access the various data-sets in different capabilities and maintaining the reliability and honesty of such data-sets, the security requirement is the important part. In this paper the main point emphasized is security of user's information. This research paper focuses on privacy & security of information access and maintaining the reliability and honesty of information being accessed in cloud platform by using data hiding methods. So in our proposed framework ;First initially user-owner encrypted the original Image-data before uploading to cloud. Once the Image-data is encrypted and uploaded to cloud, this encrypted image i.e. cipher-text image in cloud computing platform, is splitted into two equal parts i.e. equal halves as shown in figure-6. The First-half part image is focused to steganography by using Least-Significant-Bit (LSB) and RGB displacement method both together. And the Second-half part image is focused to Watermarking technique using Elliptic-Curve-Cryptosystem algorithm [6].

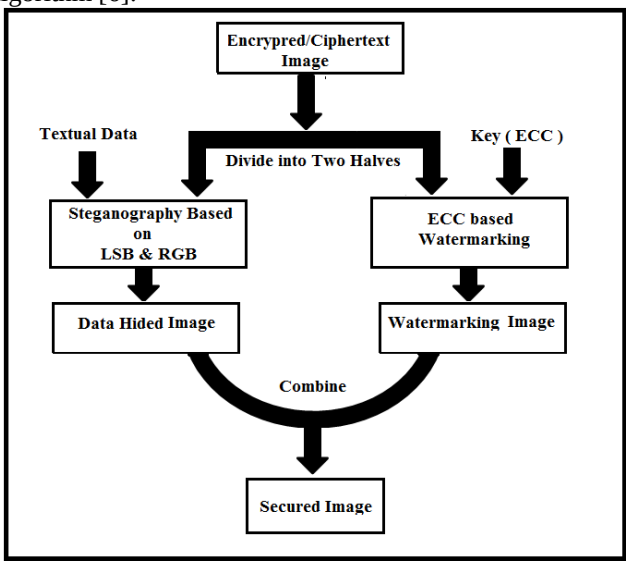

Fig. 6. Framework in Cloud

The First-half part of image is focused to RGB-LSB method of steganography. This is one data hiding method which hides LSB (List Significant Bits) of every pixel in Image-data. Now Secret message of textual data randomly generated in cloud server platform is shuffled and converted to binary bits. Then these bits are inserted in Red, Green, and Blue Least Significant Bits of every pixel in First-half part of Image-data. Now the secret message is embedded in RGB components of Image-data, which is very difficult to break and also difficult to predict the secret message data by the interloper. This is the procedure of getting First-half-stegno image [6].

The second-half part of the encrypted image is focused to a secure watermarking technique by using ECC (Elliptic curve cryptosystem) algorithm, which is most existing solution. The watermarking technique is to protect the secret Image-data from being tampered. In ECC algorithm, there is a public-key-cryptography which is based on algebraic organization of elliptic curves over finite domain fields. In the ECC the security depends on the multiplication-computing point's ability. When this ECC algorithm is compared with RSA algorithm, we observed that the smaller Key-Size is holded by ECC algorithm, with reduced size storage. Here in ECC algorithm, the public-key obtained is used for embedding watermark into Image-data. After this cloud server in cloud computing platform generates the private-key and public-key by using ECC algorithm. These keys generated are taken as location-point situation in an image and cloud server generates the watermarked Image-data.

In cloud computing platform, once the stegno-image is generated by steganography method and Watermarked-image is

generated by the watermarking techniques; which are applied on splitted two equal-half parts on an encrypted-image respectively. Then the stegno-image and the watermarked image are collectively combined to generate a Secured-Image in the cloud computing platform.

After that in cloud computing platform, the cloud server precedes the demanded results back in cipher-text Image form, given in figure-7, to the User or User-owner, by applying decryption method on secured-image in cloud; which is just reversing the process of encryption method

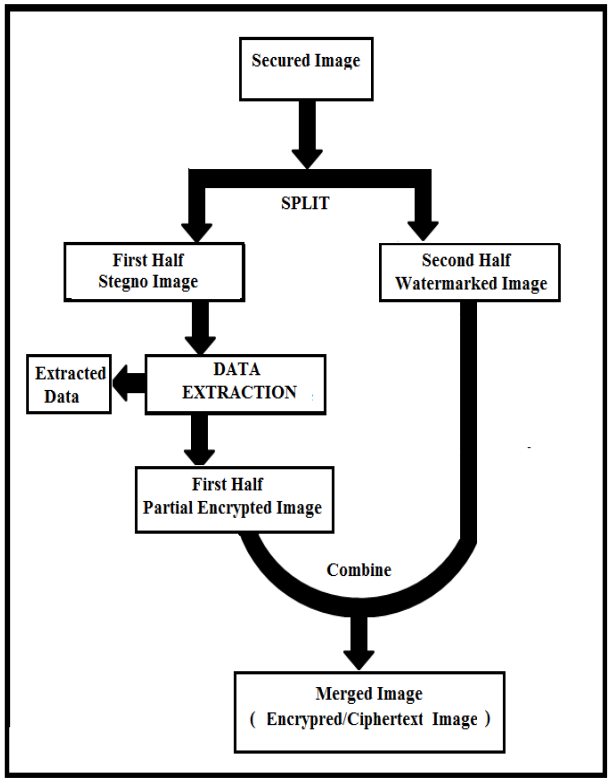

Fig. 7. Retrieval of Frame-work in Cloud

Then finally decryption process in figure-8, is done by the User using RGB pixel displacement Decryption to get the Original Image as shown in figure-9

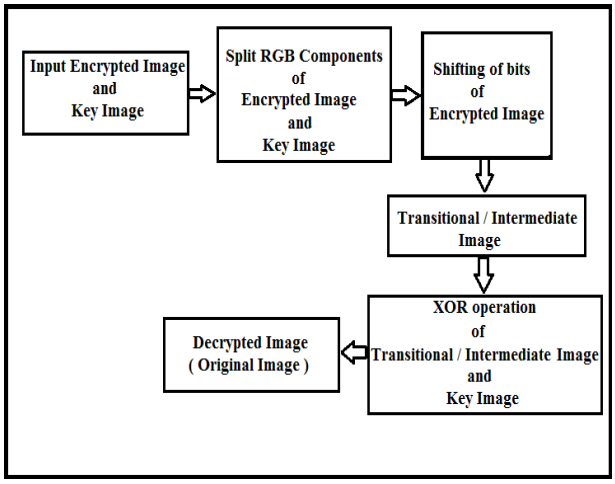

Fig. 8. RGB pixel displacement Decryption

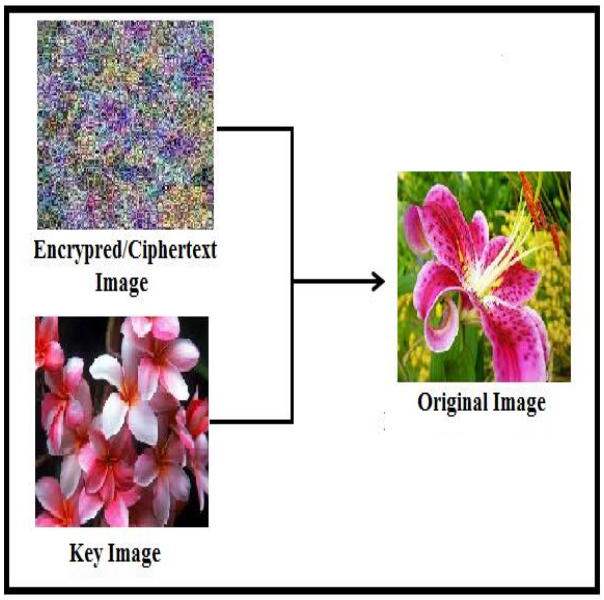

Fig. 9. Regeneration of Original Image by User

V. RESULTS

In our proposed framework, following steps given below are involved in the entire process using MATLAB. In this we out-line a table-1 which describes the each step output of the processed involved in proposed framework.

1. First the Input image is taken by the user.
2. The given Input Image is encrypted before uploading on Cloud by User and named as Cipher-text Image.
3. Now this cipher-text image which is uploaded on Cloud-platform is splitted into two equal parts by cloud-computing process in cloud itself.
4. First half part image is focused to steganography by using LSB and RGB displacement method both together and named as stegno-image.
5. Second half part image is focused to water marking technique using ECC algorithm.
6. Then both the stegno-image and watermarked image are combined to get the secured-image in the cloud computing platform.
7. After that, in cloud computing platform, the cloud server precedes the demanded results back in cipher-text Image form when required (i.e. means if cloud needs to retrieve the original cipher-text Image then the secured-image is again splitted into two parts, from the first part of image ,steganography is removed by extracting the textual data from the image and the second part the process of Extracting watermark done by reverse the embedding algorithm, in the cloud platform and then after this both extracted images are added together to form cipher-text image.).
8. If the data owner wants to retrieve the original image then he/she decrypted the cipher-text image to get the original image.

Table-1: Results of the Image Generation in entire process.

Input Image by User (original Image)	
Encrypted /Cipher-text Image	
First Half part of Cipher-text Image (in Cloud Computing Platform)	
Second Half part of Cipher-text Image (in Cloud Computing Platform)	
Steganography of First Half part of Cipher-text Image (in the Cloud Computing Platform)	
Watermarking of Second Half part of Cipher text Image (in the Cloud computing Platform)	
Merge Image (First part of Steganography and Second part of Watermarking both merged in Cloud Computing platform and stored in Cloud as Secured-Image)	
Encrypted / cipher-text Image Cloud Computing Platform returns the requested results in the form of ciphertext back to owner user	
Decrypted the cipher-text image by User (which is received by User from Cloud Computing Platform) to get to get the original image.	

VI. CONCLUSION

In Image-data processing method, RGB pixel displacement algorithm is best one for encrypt the color Image-data and it is also suitable for encrypt 3D images data. This proposed system stresses on generating key-based on color images and the single-key is used for encryption & decryption. In this, there is no need for User to remember the keys and prevents the key loss. So it is observed that, this method of cryptography is more efficient, reliable and provide more security.RGB pixel displacement has been preferred for encryption-decryption operation at higher speed.

Presently in Internet-Technology, Cloud computing is providing much dominated innovation role. So here again security and privacy enhanced methods required. In this cloud platform, the privacy of an embedded message is improved by data-hiding methods and ECC based watermarking technique manipulates copyright protection, to make sure that no intruder can own the data.

In our research work, we observed that an encrypted image i.e. cipher-text image is created and performing encryption-decryption at User level. Data hiding and ECC based watermarking technique at cloud computing platform with reduced time. We also observed when the Image-data owner or user retrieves the Image-data, then there is no-effect of change, on the quality of Image-data, thus keep original Image-data preserved

Our both proposed algorithm at user level and cloud computing level is helpful for the today's requirement.

REFERENCES

1. Zhan Qin, Jingbo Yan et al. "Privacy-preserving Outsourcing of Image Global Feature Detection", Global Communications Conference GLOBECOM), 2014 IEEE, 710-715.
2. Murat Yesilyurt and Yildiray Yalman,"New approach for ensuring cloud computing security: using data hiding methods", Sadhana, Journal of the Indian Academy of Sciences, November 2016, Volume-41, Issue 11, pp. 1289–1298.
3. Zhan Qin, et al." Privacy-Preserving Image Processing in the Cloud", IEEE Cloud Computing, Issue No. 02, vol. 5, (2018):48-57.
4. Cong Wang , Bingsheng Zhang, et.al," Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud" , IEEE Transactions on Cloud Computing , vol:1, no:1 2013.
5. Boddu Ramya Sri, Shrija Madhu, et. al. "A Novel Method for Encryption of Images based on Displacement of RGB Pixels", International Journal of Trend in Research and Development (IJTRD), Special Issue | NCETC-17, April 2017pp: 4-7.
6. M. Thangavel, P. Varalakshmi et. al. "SMCSRC – Secure Multimedia Content Storage and Retrieval in Cloud", Fifth International Conference on Recent Trends in Information Technology, 2016 pp.: 1-6.
7. Dipti Rao, Muzammil Hasan "Secure Multimedia Data Storage in Cloud Computing ", International Journal of Engineering Sciences & Research Technology, 6(5): May, 2017 pp: 391-395.
8. S. Udhayavene, Aathira T. Dev and K. Chandrasekaran "New Data Hiding Technique In Encrypted Image: DKL Algorithm (Differing Key Length)", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), ScienceDirect Procedia Computer Science 54 (2015) 790 – 798.
9. Craig Gentry, Shai Halevi and Nigel P.,"Smart, Homomorphic Evaluation of the AES Circuit", Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology --- CRYPTO 2012 - Volume 7417 Pages 850-867.
10. Priyanka Gupta, Amandeep Kaur Brar "An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server", International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, Jul-Aug 2013, pp.2273-2277.
11. Debasis Das," Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", IEEE International Conference on Information Networking (ICOIN), pp: 391-396, 10-12 Jan. 2018.
12. Murat Yesilyurt and Yildiray Yalman," New approach for ensuring cloud computing security: using data hiding methods", Sadhana November 2016, Volume 41, Issue 11, pp 1289–1298.
13. D. Chandramohan et. al. "A new privacy preserving technique for cloud service user endorsement using multi-agents", Journal of King Saud University – Computer and Information Sciences (2016) 28, pp: 37–54.
14. Ali Gholami et. al. "Privacy Threat Modeling for Emerging BiobankClouds", International Workshop on Privacy and Security in HealthCare 2014 (PSCare14), Procedia Computer Science 37 (2014) pp: 489 – 496.
15. Chao-Yung Hsu et. al. "Image Feature Extraction in Encrypted Domain with Privacy-Preserving SIFT", IEEE Transactions on Image Processing, Vol. 21, No. 11, November 2012, pp: 4593-4607.
16. Naik Riddhi and, Nikunj Gamit, "An Efficient Algorithm for Dynamic Key Generation for Image Encryption", IEEE International Conference on Computer, Communication and Control (IC4-2015). 10-12 Sept. 2015.
17. Zhan Qin, et. al. "Towards Efficient Privacy-preserving Image Feature Extraction in Cloud Computing", Proceedings of the 22nd ACM international conference on Multimedia November 03 - 07, 2014, Pages 497-506.
18. Yifeng Zheng, et. al. "Privacy-Preserving Image Denoising From External Cloud Databases", IEEE Transactions on Information Forensics and Security, Volume: 12 , Issue: 6 , June 2017, pp: 1285-1298.
19. Yifan Tian, et. al. "CAPIA: Cloud assisted privacy- preserving image annotation", IEEE Conference on Communications and Network Security (CNS), 9-11 Oct. 2017.

20. Geeta C M, et. al., "Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions", International Journal of Computer (IJC), (2018) Volume 28, No 1, pp 8-57.
21. M. Tarek Ibn Ziad, et . al. "CryptoImg: Privacy Preserving Processing Over Encrypted Images", 2nd IEEE Workshop on Security and Privacy in the Cloud (SPC 2016), 17-19 Oct. 2016.
22. Zaid Ameen Abduljabbar, et. al. "Privacy-preserving Image Retrieval in IoT-Cloud", EEE Trustcom/BigDataSE/ISPA, 2016.
23. Caihui Lan , et. al." A New Security Cloud Storage Data Encryption Scheme Based on Identity Proxy Re-encryption", International Journal of Network Security, Vol.19, No.5, Sept. 2017, PP.804-810.
24. Zhihua Xia, et. al. "Secure Image LBP Feature Extraction in Cloud-Based Smart Campus" ,IEEE Access Special Section on Novel Learning Applications and Services for Smart Campus, volume 6, 2018,pp: 30392-30401.
25. Haihua Liang, et. al. "Secure and Efficient Image Retrieval over Encrypted Cloud Data", Hindawi Security and Communication Networks, 2018, pp: 1-14.
26. Shen E, Varia M, Cunningham RK, Vesey WK. Cryptographically Secure Computation, IEEE Computer Society, Vol. 48, No.4, 2015, pp. 78–81.

AUTHORS PROFILE

Jitendra Kumar Gothwal is Professor of Computer Science & Engineering Department at Rajeev Gandhi Memorial College of Engineering & Technology (AUTONOMOUS) at Nandyal, Andhra Pradesh, INDIA. He received his B.E. in Computer Science & Engineering from University of Rajasthan, India and M.Tech.in Computer Science & Engineering from Kurukshetra University Kurukshetra, India. He also obtained Ph.D. in Computer Science & Engineering from SRU, Alwar Rajasthan, India. His Current Research intent includes Cloud Computing and Security, Bio-metric Authentication System design, Image Processing and Artificial Intelligence. He has published many research papers in National and International Journals as well as in conferences. He is reviewer of many National and International Journals.

Kunam Subba Reddy after completing B.Tech and M.Tech in Computer Science and Engineering. He obtained Ph.D. in Computer Science & Engineering from JNTU Anatapuramu under the guidance of Dr. V Vijaya Kumar, Director – Center for Advanced Computational Research (CACR) of AGI (Autonomous), Hyderabad, India and He is currently working as a Professor at Rajeev Gandhi Memorial College of Engineering & Technology (AUTONOMOUS) at Nandyal, Andhra Pradesh, INDIA, with an overall teaching experience of 20 years in various positions and published more than 30 research publications in National and International Journals as well as in Conferences also He is IEEE Senior member.