International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 11 (2019) pp. 2559-2569

A Multi-Level Security Framework on Crypt Images in Private Cloud

[1]Ms. Lavanya Kandikunta, [2]Mrs. B. Hari Chandana, [3]Prof. T. Bhaskar Reddy

[1, 2, 3]Department of Computer Science and Technology, Sri Krishnadevaraya University Anantapur-515003, Andhra Pradesh, India.

Abstract

An organization's security policies and data management determines the safe and secure- work environment. Multi-National companies, Defence, Intelligence Bureau and National-Security organisations still find difficulty in securing data from falling prey to the hackers and Spy threats. So far, we have the best Cloud Computing Services where the Secret data transactions can be done safely within the organizations. But Data Security out of an organization has been a biggest challenge to the Organizations, where data to be confidential and restricted. Nevertheless designing a proper Cloud computing Architecture with Virtual Private Cloud(VPC) will help the employees to work from anywhere, lack of fear for data security threat. To overcome the security issues we proposed algorithms and policies. In this paper Subsequently we expect an Advanced Cloud Computing Services(ACCS) with two techniques, they are Image Alter Ego(IAE) and Anti Image Alter Ego(AIAE) techniques. In this context, where the mystery information like pictures, sound, video and content are pre-prepared utilizing Nested Randomization, Steganography, Compression Techniques and encryption calculations then we get incoherent images on these we are applying two techniques IAE and AIAE. Then that are securely incorporated inside the Private Cloud by applying our Proposed Data Owner's Policy (DOP) for hearty Data Security. Hence the result and analysis have proved that proposed framework is better than existing conventional methods.

Keywords: Data Security, VPC, DOP, IAE, AIAE, AWS S3, AWS Cloud, ACCS.

INTRODUCTION

Cloud Computing is nothing but a On-Demand service of Computer Power, Storage application etc; by means of internet as Pay-per-use fashion. It provides Properties like self-service and elasticity enabling users, dynamically and flexibly adjust either resources convenience based on the current workloads. Cloud Computing is delivered to users through Three major service models, four deployment models, five essential characteristics.

There are many top service provider companies in cloud computing such as Amazon Web Services(AWS), Micro-soft Azure, Rack space, Kamatera etc.; We Choose Amazon Web Services(AWS), when compared to other service providers, AWS is a safe assured cloud service platform, it will delivered over all services will the low cost, we get experience with AWS of free for 12 months. AWS is more flexible, cost-effective, reliable, highly-scalable, high performance and secure.

Global AWS Infrastructure manages 57 availability zones within the 19 geographical regions exists in the world and AWS also introducing 12 more availability zones and 4 more regions. From these regions and zones customers can store the secret data in any where globally and maintained the replicated data at any another region before Natural Disasters will occur.

Here we are using virtual private cloud[9] that involves well defined and secure cloud based ecosystem. In this cloud only one specific client can operate. Data can be shared based on restrictive conditions. So, in private cloud our data is stored secure and safe manner.

A. Image Alter-Ego(IAE)

In term Image Alter-Ego is used to refer to the different phases of an image. Here Data Owner will partition the secret images and placing into different buckets in different regions of private cloud. This technique is introduced to increase the security level, in case any hackers are robbed the data at one region he can't get the secret information from that region completely and hackers can't understand what that actual information was present in that region.

B. Data Owner's Policy

These policies are act as the barriers for unauthorized users or hackers. Login into the cloud storage and accessing our data is difficult for those who are not authenticated. It improves the security to our secret information.

C. Anti Image Alter-Ego(AIAE)

This is the reverse process of IAE, AIAE technique is used to get the secret images from different buckets at two regions a & b in the cloud. If the user must have the authentication to see the image then image in the cloud will displays.

Cloud Computing Services(CCS) are available in the digital era since many years but still we don't have efficient security as well as reliability. We've studied various service models and architectures where we can adopt our desired infrastructure with wide feather of platforms to support our applications. We have Private Cloud Compatibility to choose for activities in a period of their respective organizations for better security together with confidentiality. Cloud Computing on driving edge for IT sector has brought many benefits and it gives the utility to ingress our robust application through internet. Can configure applications by a virtue of our desired way at any time which doesn't require any software to install into our device and configure. Confinement failure is greatest hazard includes the disappointment of disengagement system that isolates stockpiling, memory, directing in between the distinctive inhabitants. The information asked for blotting out may not get erased. In fact it happens for both of the

accompanying reasons: Extra duplicate of information are put away, however that are not accessible, Disk crushed likewise stores secret data from different inhabitants.

RELATED WORK

K.Govinda and Dr.E. Sathiyamoorthy **[4],** in this paper they utilized Group Digital Signature(GDS) and executed for Identity anonymization and secure information stockpiling in private cloud. They utilized RSA calculation for producing key match and also encryption, decoding and mark. Utilizing Diffe-Hellman's calculation mystery enter is circulated in the middle of gathering administrator and cloud supplier.

A Venkatesh and Marrynal S Eastaff **[5],** in this paper they are examine distinctive strategies that are utilized for information stockpiling on cloud safely. They utilized Secure Co-Processor(SCP), it is a piece of cloud foundation, that to empower productive scrambled capacity of delicate information. By implanting this Secure Co-Processor, the framework can deal with scrambled information proficiently. In the event that any altering is identified, SCP clears the interior memory. So it is temper-opposition.

Pooja Bandal1, Ashwini Dhane2, Shubham Chavan3, Prof. Nilima Nikam4 **[6],** the protection safeguarding productive casing work is done based on Diffie-Hellman message trade convention that gives certain security certification to client and furthermore join office for the client in the cloud.

Rongzhi Wang **[7]** in this paper, they proposed Data Secure capacity plot Based on Tornado codes(DSBT) by joining symmetric encryption and deletion codes. The believed log is presented dependent on POR calculation and BSL short signature. At last, they joined with DSBT Scheme, to upgrade the computational proficiency of the POR calculation.

DESIGN AND METHODOLOGY

A. Proposed Technique:

The proposed methodology has three important aspects. The first is data owner aspect, in this the secret data is stored by the data owner in the private cloud. The second is cloud aspect, in this the secret data is maintained and data is provided to particular authenticated user. The third is user aspect, how and where the secret data is to be gathered.

Design flow of proposed work:

1. Data Owner - design flow:

In the first proposed method where images can be pre-processed using steganography, nested-randomization and Forecast lossless-compression techniques as in Figure 1 and in other proposed method where images can be pre-processed using Steganography and Run-length encoding techniques shows in Figure 2. First take compressed images and apply the segmentation technique of N*N blocks for the encrypted image and place the N*N blocks in cloud Amazon S3 data storage.

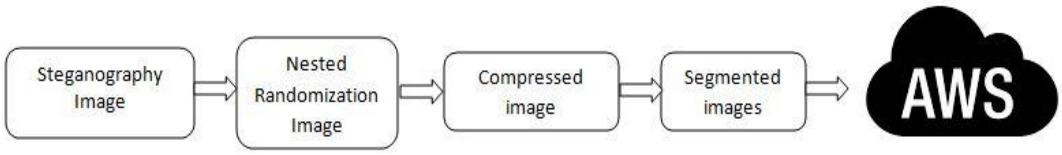

Figure 1: First method placed in AWS cloud

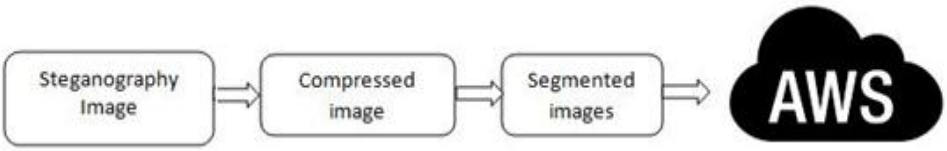

Figure 2: Second Method placed in AWS cloud

Reconstruction technique and Data Owner Key(DOK) is provided to cloud as shows in Figure 3,it will encrypt the data using DOK. Here password is treated as DOK.

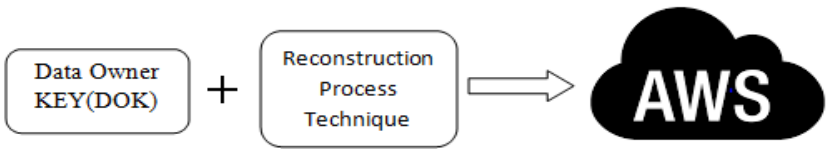

Figure 3: Reconstruction Process placed in AWS cloud

2. Cloud - design flow:

In Figure 4 Amazon S3 Web Service will generate the symmetric key for compressed image and encrypt compressed image with the symmetric key and stored in Amazon S3 Storage as blocks of images. Amazon S3 Web Service again encrypts the symmetric key with the master key and stores in Amazon S3 Storage. Whenever the user requests, AWS Cloud will ask for the token if user provide the token then AWS Cloud gives access to the data for that authorized user.

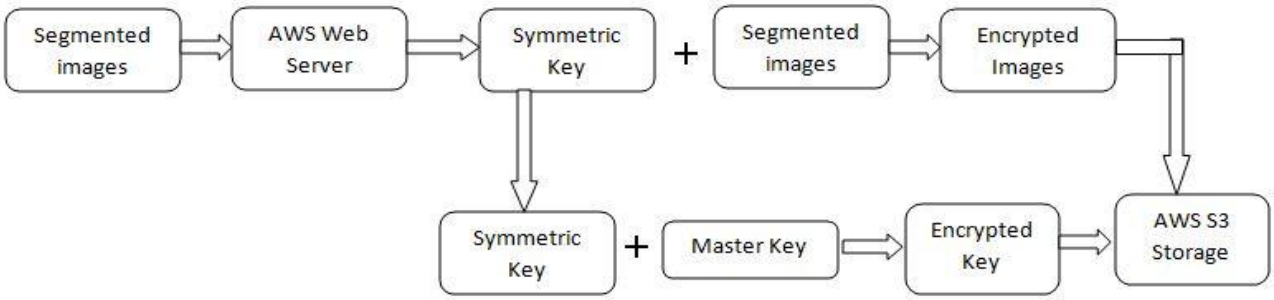

Figure 4: AWS Server Encryption

Whenever the data owner provide reconstruction technique and DOK to S3web server, it will encrypt that data and removes the DOK from the S3 storage as in Figure 5 and stores only encrypted data. User must provide the same DOK to allow S3 to decrypt. Here data owner must take care of DOK, cloud is not responsible.

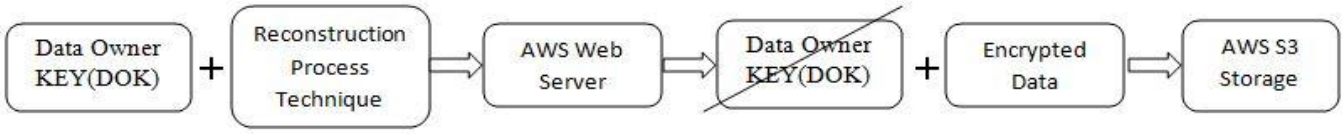

Figure 5: AWS Server Encryption with DOK

3. User - design flow:

Authorized User will request to data owner to access the data, then data owner provides DOK and Security Token to user.

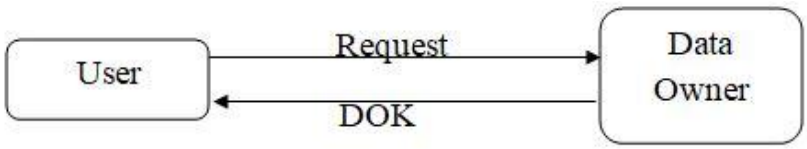

Figure 6: User Data Request

Again User must Login to AWS cloud, provide DOK and Security Token to S3 web server then Authorized user with gets the requested data from the cloud.

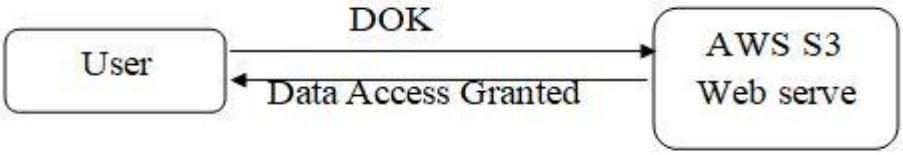

Figure 7: User Data Access Request

After this user gets compressed images 1&2 and also the reconstruction process, from this user will gets the secret images.

B. Proposed Architecture

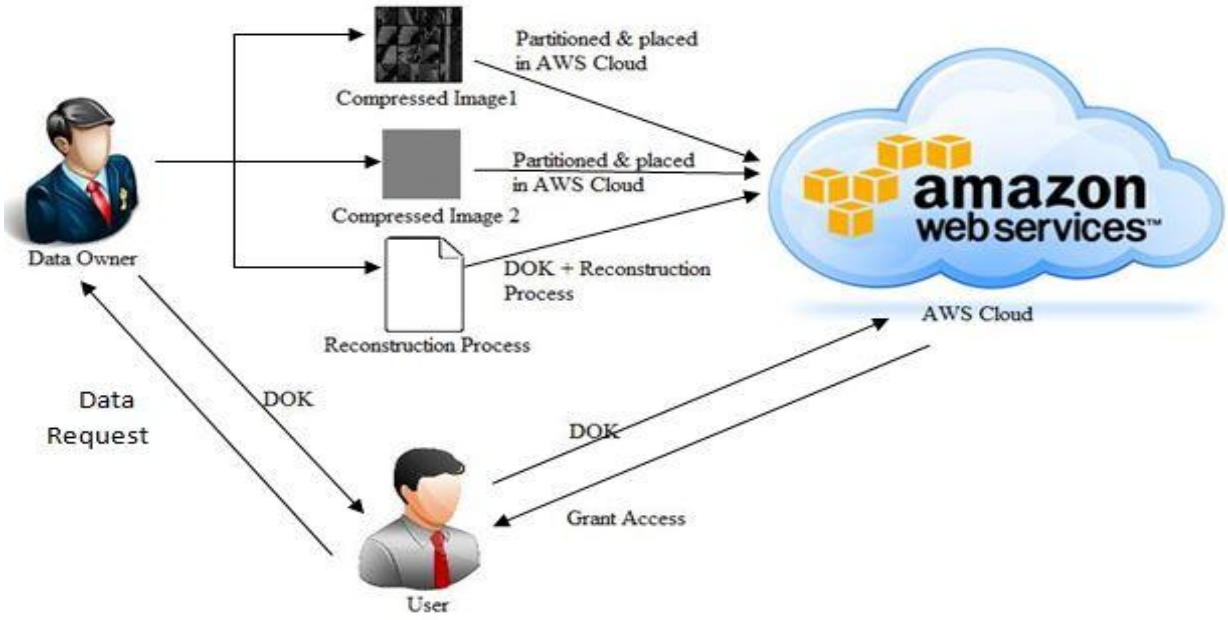

Figure 8. Overview of Proposed Work

The Secret images is processed[1] then we get Compressed images. Data owner(DO) will partitioned the Compressed images 1 into 5x5 segments and placed in to buckets using Image Alter-Ego technique at regions A first and then at region B in AWS S3. Again the Compressed images 2 will be partitioned into 5x5 segments and placed in to buckets Image Alter-Ego technique at region B first and then at region A in AWS S3. The reconstruction process for secret images with the DataOwnerKey(DOK) is send to AWS cloud, here DOK is generating using existing AES algorithm. Whenever user needs the data, user will send a Data request(DR) to DO, DO will check whether the user was Authorized User(AU) or not, then DO sends the DOK to user. Data proprietor will add the approved clients to bunches at whatever point the information demand will come. Then Authorized User(AU) provides the DOK to AWS Cloud, cloud will check either AU will follow the Data Owner's policy or not and compares AU's IP address with AU account Login IP address if it is same, then cloud will give data access to AU otherwise that IP address will be restricted. At last AU will get the needed Data. After accessing the data all connections will be detached from the user.

Steps Involved:

1) Member Login to AWS Cloud:

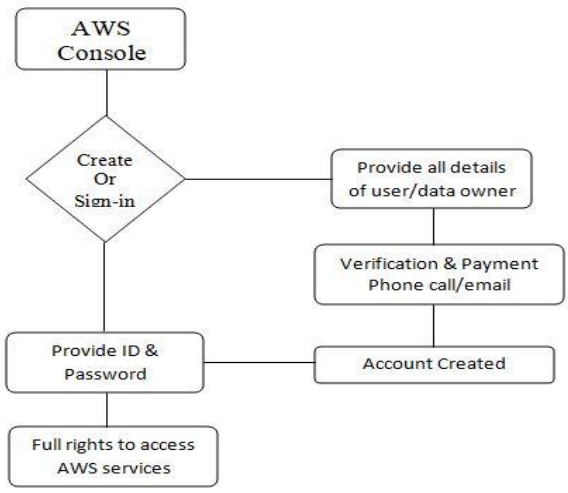

Figure 9: AWS Member Login

2) To store or retrieve the data into AWS cloud first we need to create the aws account if you are the first time user/data owner, provide your details. Otherwise directly sign into the aws account and get access to AWS services.Creating AWS EC2 Instance:

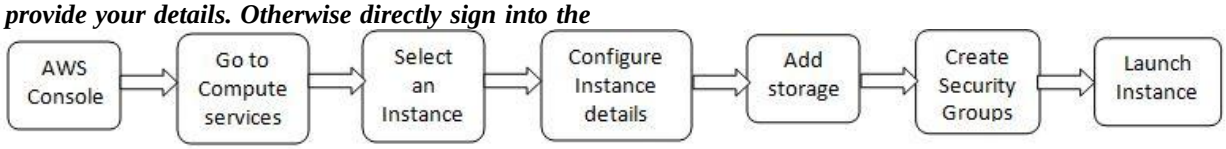

Figure 10: AWS EC2 Instance Creation

3) To create AWS EC2 instance as shown in figure 10, we have to select what type of instance to be created and configure instance details, add the storage type, create user/default security groups finally launch the instance.IAM(Identity Access Management):

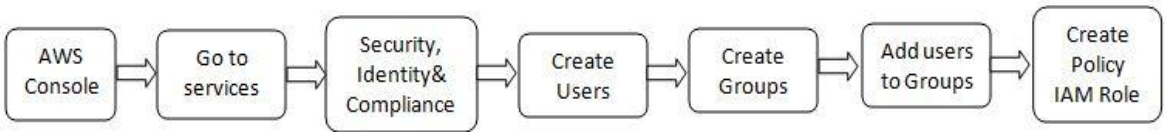

Figure 11: IAM Creation

After Launching Instance we will use IAM(Identity Access Management), it enables security control access to AWS services and resources for our users. Using IAM we can create and Manage AWS users and groups, also use permissions to allow and deny their access to AWS resources. It has feature of our AWS accounts offered at no additional charge you will be charged, only for use of other AWS services by our users will be charged.

Features:

- Shared access to our AWS accounts.
- Granular Permissions.
- Identity Federation.
- Create and manage users, groups, policies to grant access 1to AWS services & resources.

4) VPC(Virtual Private Cloud):

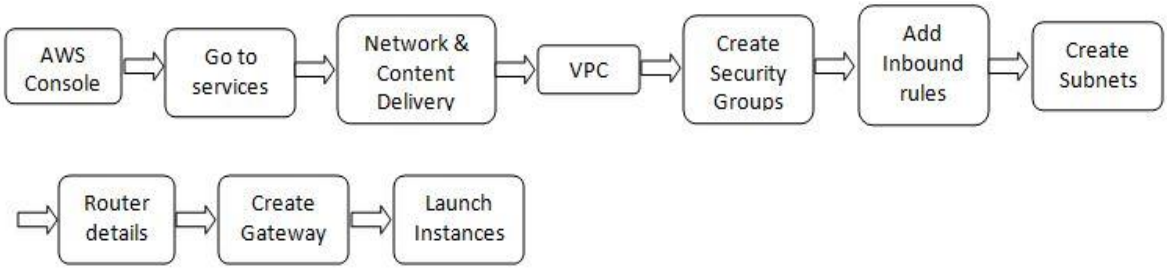

Figure 12: VPC Creation

With in Public Cloud Environment, A VPC [9] is a on-demand configurable pool of shared computing resources. By providing certain level of restrictions in between the different organizations. VPC is a virtual network that is provided to your AWS account, it is logically unique from all other networks in AWS cloud. You can Launch your AWS resources(Amazon EC2 Instances) in to your VPC.

To your VPC

- Specify an IP address range.
- Add subnets.
- Assigning Associated Security Groups.
- Configure Route Tables.

The Main use of Security Groups is, it acts as a virtual firewall to control the incoming traffic of associated Instances, by adding the inbound rules we can also control the incoming traffic. By default VPC will creates the default Security Group at the time of creating VPC. We can use default Security Groups or we can create new one i.e; WebServerSG. When you Launch Instances to your VPC then specify this Security Group.

5) Here we are launching EC2 Instance same as we discussed earlier but in the organization's private network by choosing newly created VPC, subnets, Route Tables, Internet Gateways and applying their own Security Groups, restriction, we can give our data at the time Instance creation or after the Instance creation, adding storage etc, to that

particular Instance and Launch.Storing the DATA into AWS Cloud S3(Simple Storage Services):

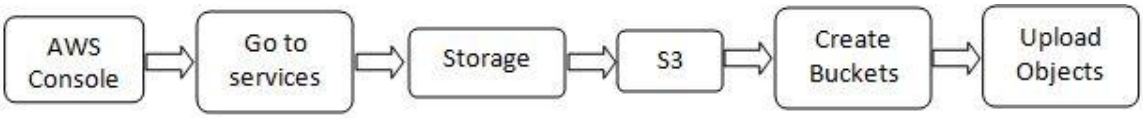

Figure 13: Object Creation & Storing

We are storing our resulted compressed images into AWS S3[10]. Before that we need to create a Bucket. Globally Buckets are unique containers you can store everything in AWS S3. Sign-in to AWS Console,Storage,S3. There we get Create a Bucket, Delete Bucket, Empty Bucket. If you are not created any Bucket till now then you need to click on "Create Bucket". Then it will select the default region which we have the AWS account or we can select in different region at the time of bucket creation. Click on Next Button then it will check the bucket name if it exist, then you need to change the name. Then you will "Configuration Option" there you have to give the details like Versioning, Default encryption etc, click on Next. You get "Set Permissions" here you can multiple accounts and Object permissions are private by default, but you can setup access control policies to grant permission to others (like read and write permissions, access rights like public or system), then click Next. You get "Review" here you can edit, if anything want to modify, if not click on "Create Bucket". Then it will create the bucket, this bucket is empty we need to add the data(images, files, documents, audio & video files) in the form of Objects.

C. Proposed Data Owner's Own Policy:

- User must provide all details to the organization.
- Data Owner should check whether the user is trusted user or no.
- If the user is trust user, data owner will give access to the user by creating ID& Password. The user must change the password after the first login.
- For every Six months user must change the password for security, if not cloud will send notifications to that particular user.
- If user did not change the password after the intimation, user registration will be cancelled.
- Authentication is verified for every data transfer.
- The data provider give access to the authorized person for particular point of time, after that user cannot access the data.
- The data is supported to authorized person's IP address only.
- No Other IP address will allow in to the network without any authorization.
- If the user want to change the IP address or user the person wants the data to another IP, that person again wants to take authentication to that particular IP address from the cloud.
- The provider wants to check what that authorized person was doing with the data.
- While accessing the data, in case user is in deactivate state after some period of time, session timeout will be raised and all resources & accessing rights will be detached from the user.
- If that person is misusing the data at that particular point of time the authorized person authentication will be cancelled.

D. Proposed Algorithms and procedures

1) Image Alter-Egotechnique:

Here we have 2 compressed images. Each image is segmented into 5x5 segments, then we get 25 segments and name them as Compressed1part [i],Compressed2part[i], here 'i' represents the image segment numbers(0-24). Each segment is placed in buckets in AWS S3. Before Storing in AWS S3, we need to create 25 buckets in 2 regions(a,b), each region contains 25 buckets and name them Region(a)bucket[j], Region(b)bucket[j], here 'j' represents bucket numbers(0-24). Take the Compressed1parts[i] and store in to the buckets in region(a&b) alternatively. i.e; Take first part from 1st image and store in the 1st bucket at region-**a**, and take the 2nd part from 1st image and store in the 2nd bucket at region-**b**, same procedure will apply to all parts, till all image parts are completed. Repeat the same procedure for Compressed2parts[i], but here regions should be interchanged. i.e; 2nd image 1st part is stored in the 1st bucket at region-**b** first then the 2nd image 2nd part is stored in the 2nd bucket at region-**a**.

Algorithm1 using Image Alter-Ego Technique1 For Compressed image1:

Compressed image-1 Segmentation and Storing in to buckets Altenatively

Step.1	Read the input image Compressed image 1.
Step.2	Divide the image into Crows and Ccols.
Step.3	Calculate the total height and width of input image1.
Step.4	Get the width and height of each segment to divide and store in an array.
Step.5	Fetch the segmented image files from the array and store these into different buckets in region **a** first and then in region **b** alternatively.

Algorithm 2 using Image Alter-Ego Technique 2 For Compressed image2:

Compressed image-2 Segmentation and Storing in to buckets alternatively

Step.1	Read the input image Compressed image 2.
Step.2	Divide the image into Drows and Dcols.
Step.3	Calculate the total height and width of input image2.
Step.4	Get the width and height of each segment to divide and store in an array.
Step.5	Fetch the segmented image files from the array and store these into different buckets in region **b** first and then in region **a** alternatively.

2) Anti Image Alter-Ego

The reverse procedure of IAE, here we are retrieving compressed images 1& 2 from private cloud. This technique is available for data owner and who are authenticated to that particular private cloud.

Algorithm 3 for Anti Image Alter-Ego Technique:

Retrieving Compressed images from cloud using Anti Image Alter-Ego Technique

Step.1	Initialize two arrays.
Step.2	Get the image 1parts from region **a** and region **b** alternatively and store into an array Compressed 1[ ].
Step.3	Get the image 2parts from region **b** first and then region **a** alternatively and store into an array Compressed 2[ ].
Step.4	And forming two compressed images from the arrays Compressed1[ ] and Compressed2 [ ].

On these two images User will apply reconstruction process[1], thenUser will get the secret images.

RESULTS AND DISCUSSION

The implementation of proposed work is done using two Compressed images, One contains 2 secret images, other contains 8 secret images.

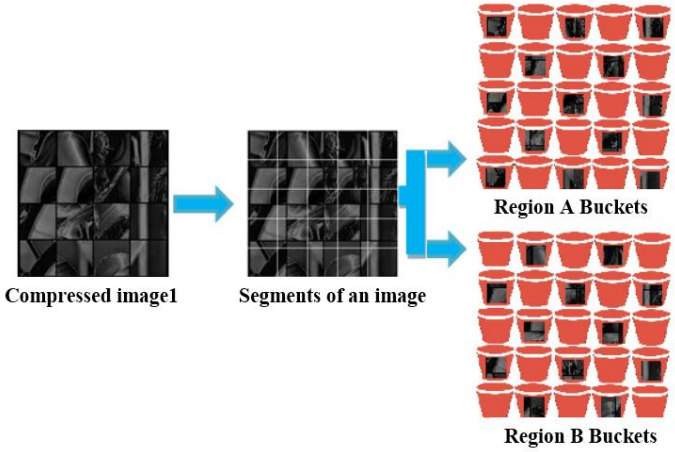

Figure 14: Compressed Image-1 storing in Cloud

The secret images are pre-processed then we get Compressed image-1, we are segmenting the compressed image-1 into 5x5 segments, that segments are placed in AWS S3 buckets at two region A&B by using Image Alter Ego technique as we explained in our proposed work.

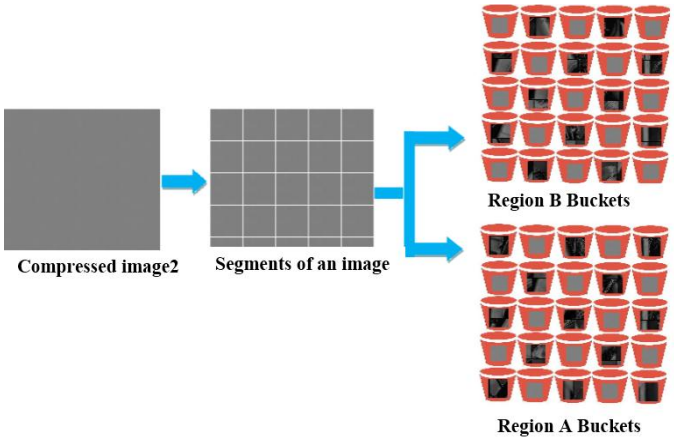

Figure 15: Compressed Image-2 storing in Cloud

It is the 2nd compressed image which is segmented in 5x5 segments and placed in AWS S3 buckets at two regions B&A. Here we placed first segment placed in region-B and then region-A.

By using Anti Image Alter Ego technique we are extracted images from two regions A&B we Compressed images back and applying Reconstruction process[1] on that two images then we get 2 secret images from compressed image1 and 8 secret images from compressed2. In case we change the segments we cannot retrieve the secret images.

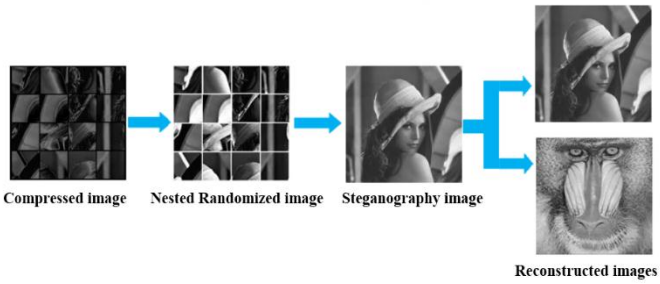

Figure 16: Reconstruction Process For Compressed image 1

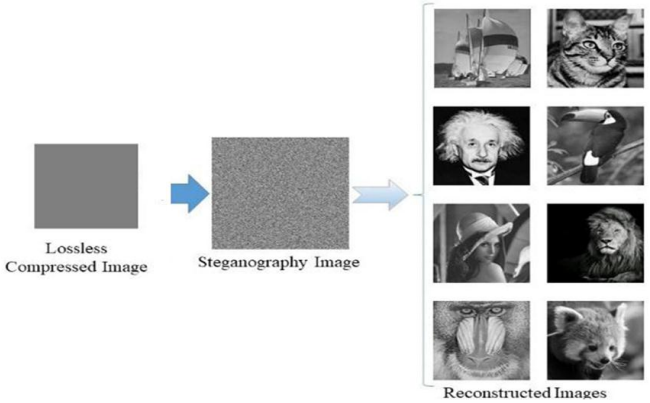

Figure 17: Reconstruction Process For Compressed image 2

HISTOGRAM ANALYSIS

Histogram analysis and comparion of Original Secret images with reconstructed secret images. By the inverse process we obtained Reconstructed images almost exactly same as orginal images, but there is no loss of occult information.

Histogram Analysis for two secret images in Compressed image1:

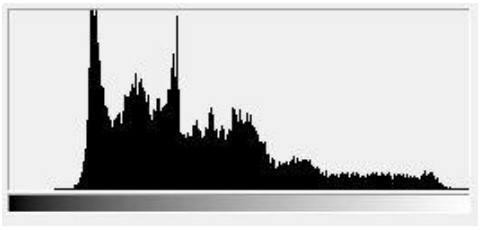

Figure 18: Original lenna

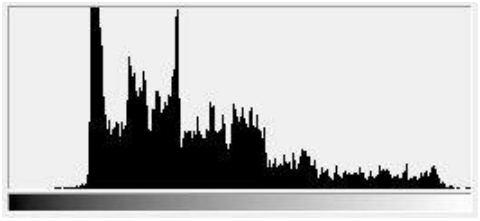

Figure 19: Reconstructed lenna

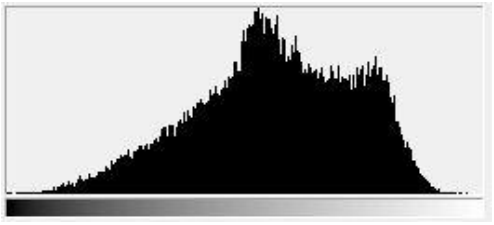

Figure 20: Original baboon

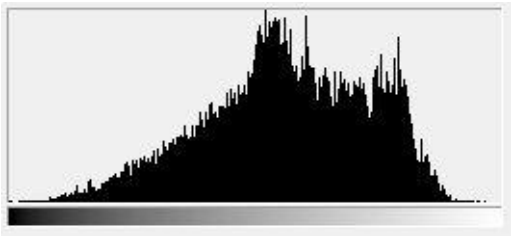

Figure 21: Reconstructed baboon

Histogram Analysis for eight secret images in Compressed Image2:

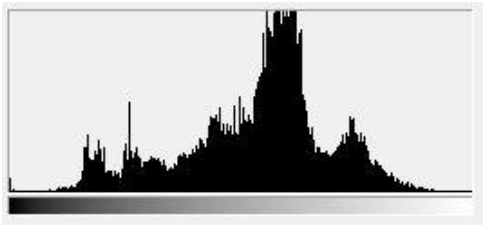

Figure 22: Original boats

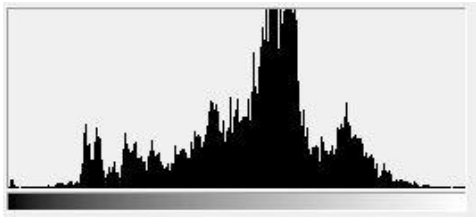

Figure 23: Reconstructed boats

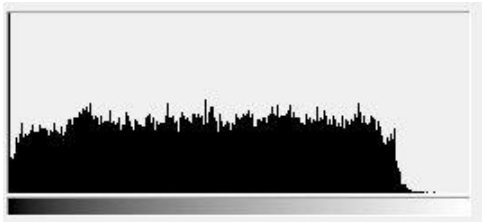

Figure 24: Original cat

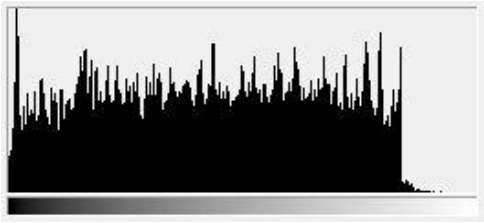

Figure 25: Reconstructed cat

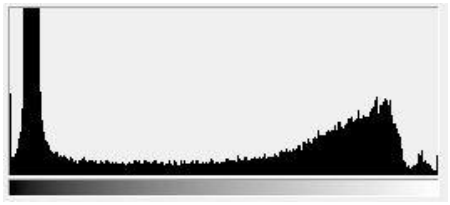

Figure 26: Original enistein

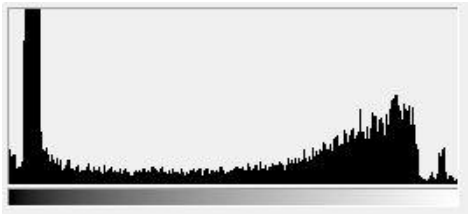

Figure 27: Reconstructed enistein

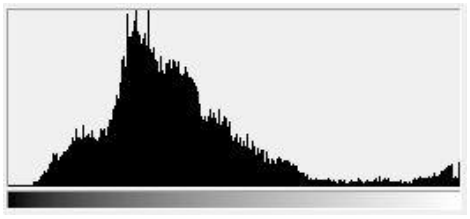

Figure 28: Original bird

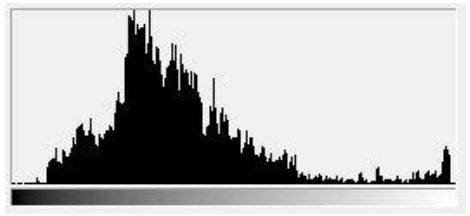

Figure 29: Reconstructed bird

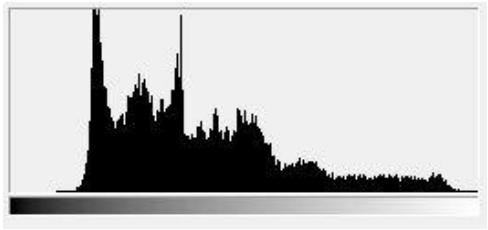

Figure 30: Original lenna

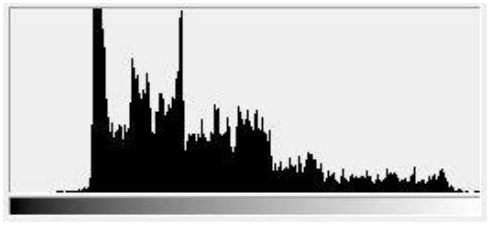

Figure 31: Reconstructed lenna

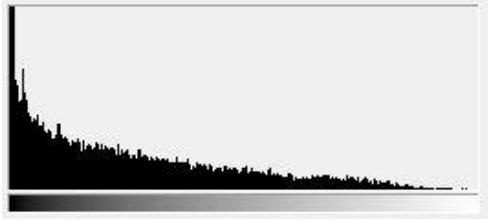

Figure 32: Original lion

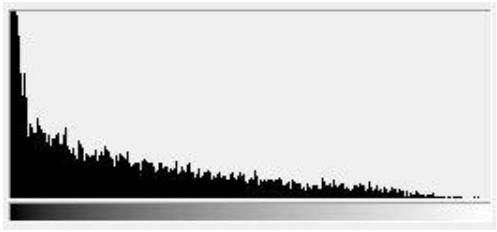

Figure 33: Reconstructed lion

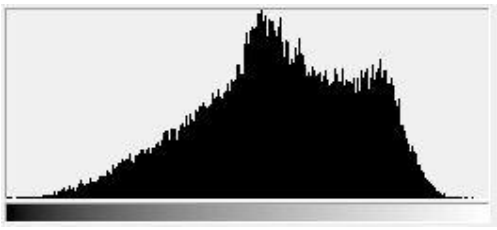

Figure 34: Original baboon

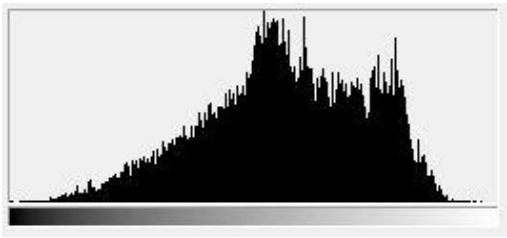

Figure 35: Reconstructed baboon

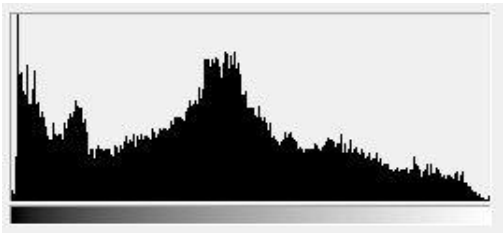

Figure 36: Original red panda

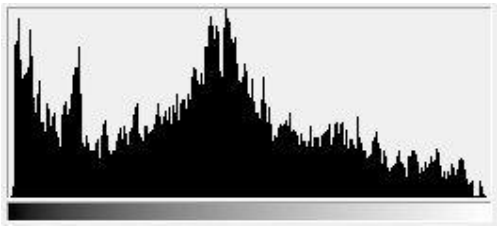

Figure 37: Reconstructed red panda

CONCLUSION

In this paper we proposed Data Owner's Policy to restrict Unauthorized IP address to improve the security level to the Private cloud, thenImage Alter Ego and Anti Image Alter Ego techniques are introduced to provide Robust Data Security to our secret image. So that by using proposed techniques, policy

and image perocessing techniques[1], no hackers or any unauthorized persons can't get any secret images from cloud. To implement more security levels on Scecret images using Security Based technologies that are useful to not only specific organisation but also for all organisations.

REFERENCES

[1] Data Security Using Nested Randomization and Lossless Compression Techniques by LavanyaKandikunta, B.Harichandana, Prof. T. Bhaskara Reddy International Journal of Applied Engineering Research. ISSN 0973-4562 Volume 13,Number 15(2018)pp. 12373-12378.

[2] COMPUTATIONALLY EFFICIENT SECURE AND PRIVACY PRESERVING STORAGE OF IMAGE DATA ON HYBRIDE CLOUD by K.Bhargavi, Prof.T.Bhaskara Reddy Journal of theoretical and Applied Information Technology 31st july 2018—Vol. 96. No.14 – 2018.

[3] AHybrid Multi-Stage Methodology for Secure Outsourcing of Confidential Data to Public Cloud by K.Bhargavi, Prof.T.Bhaskara Reddy International Journal of Computer Sciences and Engineering E-ISSN: 2347-2693 Vol.-6, Issue-6, june 2018.

[4] Identity Anonymization and secure Data Storage using Group Signature in Private Cloud by K. Govinda, Dr.E.Sathiyamoorthy https://www.sciencedirect.com/science/article/pii/S2212017312003581.

[5] A Study of Data Storage and Security Issues in Cloud Computing by A Venkatesh, marryan S Eastaff International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307.

[6] Key Exchange Privacy Preserving Technique in Cloud Computing by Pooja Bandal, Ashwini Dhane, Shubham Chavan, Prof. Nilima Nikam International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

[7] Research on Data Security Technique based on Cloud Storage by Rongzhi WangProcedia Engineering 174 (2017) 1340 – 1355

[8] AWS Cloud Computing https://aws.amazon.com

[9] Amazon Virtual Private Cloud User Guidehttps://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf#what-is-amazon-vpc

[10] Amazon Simple Storage Service Console User Guidehttps://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html

[11] A Novel Approach of Lossless Image Compression using Hashing and Huffman Coding Authors Mrs. T. Anuradha Dr. T. Bhaskara Reddy , Miss. Hema Suresh Yaragunti ,,Dr. S. Kiran Publication date 2013 Journal International Journal of Engineering Research & Technology (IJERT) Volume 2 Issue 3 Publisher ISSN: 2278-0181.

[12] Hidden security features for the recognition of fake currency by B.Harichandana, Lavanya.K, Prof.T. Bhaskara Reddy International Journal of Advanced Research in Computer Science. Mar/Apr2018, Vol.9 Issue 2, p292-299. 8p.

[13] A Novel Approach of Lossless Image Compression using Hashing and Huffman Coding Authors Mrs. T. Anuradha Dr. T. Bhaskara Reddy , Miss. Hema Suresh Yaragunti ,,Dr. S. Kiran Publication date 2013 Journal International Journal of Engineering Research & Technology (IJERT) Volume 2 Issue 3 Publisher ISSN: 2278-0181.

[14] IMPLEMENTING MULTILEVEL DATA SECURITY IN CLOUD COMPUTING by Nidhi Dahiya, Sunita Rani **DOI:** http://dx.doi.org/10.26483/ijarcs.v8i8.4636International Journal of Advanced Research in Computer Science

[15] Threshold Cryptography Based Data Security in Cloud Computing by Swati Swaraj, Chaitrali Pawar , Pragati Singh, Abhilasha Pawar, vaishali suryawanshi International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072.

[16] Data Integrity and Security in Cloud Environment Using AES Algorithm by Mr.B.Thiyagarajan, Mr.Kamalakannan.R ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

AUTHORS

Ms.Lavanya Kandikunta is research scholar in the department of Computer Science Technology at S.K.University, Anantapur. She acquired M.Sc in Computer Science from S.V. University, Tirupathi.

She has 2 years of experience in teaching . Her research interest is in the field of Image Processing.

E-Mail: kandikuntalavanya@gmail.com

Mrs.B. Harichandana is research scholar in the department of Computer Science Technology at S.K.University, Anantapur. She acquired M.Sc.in Computer Science from S.K. University, Anantapur. She has 10 years of experience in teaching. Her research interest is in the field of Image Processing.

E-Mail: harichandana1983@gmail.com

Dr.T. Bhaskara Reddy is a Professor in the department of Computer Science and Technology at S.K University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K.University and He also the CSE Coordinator of Engineering at S.K.University. He has completed his M.Sc and Ph.D in computer science from S.K.University.He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17 years. He has published 55 National and International publications. 10 International conferences. 13 National conferences. One UGC Major Research Project. Attended several seminars in 3 countries. He has completed major research project (UGC).

E-mail: bhaskarreddy_sku@yahoo.co.in