Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPUTATIONALLY EFFICIENT SECURE AND PRIVACY PRESERVING STORAGE OF IMAGE DATA ON HYBRID CLOUD

[1]K.BHARGAVI, [2]T.BHASKARA REDDY
[1] Research Scholar, Department of CSE, JNTUA College of Engineering, Anantapuramu, A.P, India
[2]Professor , Department of Computer Science & Technology, SKU Anantapuramu, A.P India
E-mail: [1]bhargavikonakanti@gmail.com, [2]bhaskarreddy.sku@gmail.com

ABSTRACT

Cloud computing has changed the model of computing by providing a huge shared pool of resources to public in pay as you go fashion. The predicted growth of cloud shows promising prospects in future. However, there is privacy concern over outsourced data to cloud. This is the challenging problem to be addressed. Many researchers contributed towards secure and privacy preserving storage of data to cloud. They could provide security and privacy benefits to cloud data owners. At the same time, they are causing much overhead. For instance, most of the cryptography based solutions introduced heavy computational costs. Another problem with many existing solutions for hybrid cloud is that the overhead and cost of usage is more. To overcome these problems, in this paper, we proposed a methodology that advocates the effectiveness of using a hybrid cloud. It discriminates the sensitive information from insensitive data and stores it in private cloud while the insensitive data which is bulky is stored in public cloud. This approach has two influencing benefits. The first benefit is optimal utilization of resources over public cloud which results in saving money. The second benefit is to have high level of security as the data stored in public cloud is highly modified copy of original data and insensitive while sensitive data stored in private cloud is needed to establish original data. We proposed an algorithm to realize secure and privacy preserving storage and retrieval of image data on hybrid cloud. We built private cloud with Aneka cloud platform and used Amazon Web Services as public cloud. We built a prototype to demonstrate proof of the concept. Results revealed that our methodology provides data privacy with negligible computational cost when compared with AES. Besides it causes little delay due to the methods employed for modification of original image data.

Keywords – *Cloud Computing, Image Security, Hybrid Cloud, Privacy Preserving, Discrimination Of Sensitive And Insensitive Data*

1. INTRODUCTION

There has been rapid growth of distributed computing that is evidenced in the form of cloud computing. As multimedia objects are growing with exponential pace, they need to be handled efficiently. Local storage and computations became inadequate with the bulk of data grown. This is the reason organizations in the real world are opting for cloud computing which provides on demand computing resources in pay per use fashion [1]. However, outsourcing everything to public cloud may become costly over a period of time. To overcome this problem, it is good idea to have a locally built cloud. However, local cloud has limited resources and it cannot guarantee scalability. To overcome this problem, a hybrid cloud concept which combines private cloud and public cloud.

1.1 Hybrid Cloud

It is one of the cloud deployment models which are the combination of two or more clouds. However, the best combination is to have private and public clouds. The rationale behind this is that private cloud does not involve payment while using it. On the other hand public cloud resources are used in pay per use fashion. Private cloud is owned by an organization while public cloud is owned by cloud service providers like Amazon, Microsoft and Google to mention few. From the literature [24], it is understood that storing everything in private cloud does not make sense as the resources are exhausted soon. At the same time storing everything in public cloud causes more expenditure. Therefore a sensible approach is to have a hybrid cloud that leverages synergic benefits

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of private and public clouds. It is shown in Figure 1.

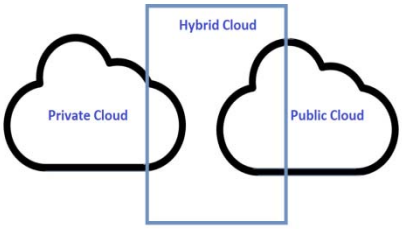


Figure 1: Hybrid Cloud Made Up of Private Cloud and Public Cloud

Hybrid cloud allows retaining sensitive data in private cloud while taking advantage of low cost and flexible storage of public cloud to hold insensitive data. Microsoft Azure, Amazon AWS, and Google Cloud are best examples for public cloud. Hybrid Cloud can be the best scenario for a cloud, since it combines the most advantages of other types. Many researchers [4], [5], [6] and [18] contributed towards exploring hybrid cloud for making a convenient and scalable means for managing multimedia objects. However, there is no light weight, secure, and privacy preserving approach to handle multimedia objects. When there is a framework to do so, it is possible that cloud usage will be increased further as there will be privacy and security to the outsourced multimedia content. This is the motivation behind the paper. The main objective of this paper is to propose and implement a framework that supports secure, privacy preserving and computationally efficient outsourcing of multimedia data to hybrid cloud. Our contributions in this paper are as follows.

- We proposed a methodology for separating sensitive an insensitive information in order to achieve secure and privacy preserving storage and retrieval of multimedia objects such as images.
- We built a hybrid cloud with locally established private cloud using Aneka [25] and Amazon Web Services as public cloud. This hybrid cloud is used to have simultaneously storing sensitive and insensitive information to private and public cloud respectively.
- We proposed an algorithm named Secure and Privacy Preserving Image Storage (SPPIS) for performing separation of sensitive data from insensitive data and achieve secure and privacy preserving image storage in public cloud. The algorithm performs shuffling, compression and converting image into text for the secure and privacy preserving storage.
- We proposed another algorithm named Secure and Privacy Preserving Image Retrieval (SPPIR) for performing operations in reverse process to obtain original image from the sensitive an insensitive data stored in private and public clouds respectively.
- We built a prototype application using Java Swing with GUI for intuitive user interface to demonstrate both secure and privacy preserving image storage and retrieval to and from hybrid cloud.

The remainder of the paper is structured as follows. Section 2 reviews literature on cloud computing, image compression, and hybrid cloud usage for image storage and retrieval. Section 3 provides the proposed system for computationally efficient image data storage and retrieval on hybrid cloud. Section 4 presents experimental results and evaluation. Section 5 provides discussion on the work done while section 6 concludes the paper besides providing directions for future work.

2. RELATED WORK

This section reviews literature on secure storage of image data in hybrid cloud and its related work. Hashem et al. [1] studied the need for using cloud computing for managing multimedia data. They also focused on the rise of big data as data is growing exponentially. They opined that large computational infrastructure is provided by cloud which is suitable for storing multimedia data and processing it. Fernando et al. [2] on the other hand investigated Mobile Cloud Computing (MCC) and its potential for working with image processing applications. They found the utility of MCC for working with image storage and retrieval. Cloud computing provides various services to its users. Giving ranking to cloud computing services and its security features can help users to choose right services. Garg et al. [3] propoed a framework named SMICloud for ranking cloud services. They used metrics to determine the ranking for services. The metrics include service responses time, sustainability, suitability, accuracy, interoperability, availability, reliability, stability, cost, adaptability, elasticity, usability, throughput and efficiency, and scalability.

Li et al. [4] explored hybrid cloud approach for secure storage of data with checking

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for duplications. It supports authorised check for duplicate copies of data with minimal overhead. Similar kind of work is done by Li et al. [18]. Zhang et al. [5] focused on proactive workload management. They formed a federation between public clouds in order to ensure scalability. They proposed a methodology for proactive management of workloads that are dynamic in nature. Sometimes, flash crowd work loads are to be handled. Lu et al. [6] studied the storage of multimedia content over hybrid cloud for increasing profit to multimedia content service providers. They proposed a framework that is used to provision multimedia services to geographically distributed users by using public cloud. They built an online algorithm that is used to manage hybrid cloud dynamics in distributed environment.

When multimedia content is stored or sent across network, compression plays an important role. Jindal [7] made a review of latest developments in image compression techniques. They explored lossless compression techniques such as run length encoding, Huffman encoding, LZW encoding, and area encoding and lossy compression techniques like transformation coding, vector quantization, fractal coding, and block truncation coding. Ram et al. [8] studied an adaptive wavelet transform technique based on path-ordering for facial image compression. They used image adaptive transform for compressing facial images. They also used sparse coding and entropy coding for effective image compression. Vijayarani and Sakila [9] investigated on document image compression with hybrid compression technique. They combined two compression techniques such as Set Partitioning in Hierarchical Trees (SPIHT) and Discrete Wavelet Transform (DWT) for better accuracy in compression. Qin et al. [10] propoed a compression technique known as joint data hiding and compression with the help of Size Match Vector Quantization (SMVQ) and image inpainting. Their approach handles both secret data embedding and compression with controlled distortion.

Tang et al. [11] employed chaotic map and block shuffling for efficient image encryption. Shuffling image blocks has its utility in adding more ssecurty to an encrypted image. Initial encryption is achieved by shuffling blocks. Overlapping blocks and overlapping sizes are used to have more efficient image encryption. To generate a set of secret matrices, chaotic map is used. Subashini et al. [12] proposed a methodology based on machine learning techniques for brain tumour grade identification. MR images are used as input for discovering tumour grade accurately based on magnetic resonant spectroscopy and biopsy. They also used Fuzzy C Means for effective segmentation.

A secure-erasure code based storage in the cloud is explored in [13] for secure storage of multimedia objects in cloud. Wang et al. [14] proposed a methodology for privacy preserving public auditing of cloud storage for security and data integrity. An effective data access control mechanism for cloud is propoed in [15]. Wei et al. [16] proposed an auditing protocol for privacy cheating discouragement. Their method supports both privacy and security to cloud storage and computations outsourced to cloud. Spillner et al. [17] proposed a cloud storage management system that combined storage facilities from multiple service providers for efficiency. Thus their work helped consumers to have flexible, secure and redundant storage features supporting other non-functional requirements like reliability.

Many researchers contributed towards securing image data in hybrid cloud. Huang and Du [19] proposed hybrid cloud for achieving big data privacy. They proposed a scheme for storing image data in hybrid cloud and besides preserving privacy of big data. They could achieve more efficiency when compared with traditional AES algorithm. Garg and Kaur [20] propoed a hybrid information security model that targets multimedia data to be stored and retrieved in hybrid clouds. They also proposed hybrid data security scheme. Sookhak et al. [21] proposed dynamic remote data auditing in cloud computing for big data security. Their auditing method employs algebraic signature properties for secure and efficient storage. The auditing method makes use of the signatures to validate the integrity of data stored data. Zhang et al. [22] on the other hand investigated and proposed a framework for secure storage and computing in hybrid cloud. They extended Map Reduce framework and named it as tagged Map Reduce for secure computing in hybrid cloud.

Yu et al. [23] proposed protocol for checking remotely stored data. They evaluated the protocol with replay and deletion attacks. They came to know that the algorithm is signature based and used to identify multimedia objects and perform possession checking. A review of multimedia content protection over cloud is made

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by Kulkarni et al. [29]. Similar kind of work is done by Manoj et al. [30]. Fotiou and Xylomenos [31] proposed an access control delegation scheme for protecting multimedia content that is outsourced to public cloud. Tayan [32] explored tools and concepts related to protection of sensitive data associated with Information Technology (IT) industry.

As reviewed above, many researchers contributed towards secure and privacy preserving storage of data to cloud and image compression technique. They could provide security and privacy benefits to cloud data owners and even exploited hybrid cloud. At the same time, they are causing much overhead. For instance, most of the cryptography based solutions introduced heavy computational costs. Another problem with many existing solutions for hybrid cloud is that the overhead and cost of usage is more. To overcome these limitations, in this paper, our approach is to use hybrid cloud with some difference. Sensitive and non-sensitive data are separated and only non-sensitive data is sent to public cloud achieving privacy and reducing computational cost.

3. EFFFICIENT IMAGE DATA STORAGE AND RETRIEVAL ON HYBRID CLOUD

3.1 System Model

The system model we considered involves both storage and retrieval of images. Computationally efficient storage and retrieval is the main focus of this research. Besides the proposed system is computationally efficient, secure and preserve privacy of data. The original data that comes from different sources is to be stored in private cloud so as to enable users of it to have access with 100% availability. The users of private cloud can access data without time and geographical restrictions. As resources are limited in private cloud, it is not wide idea to store everything in such cloud. Therefore we devised computationally efficient approach to deal with resource exhaustion and overhead problems. Storing all images in private cloud consume resources faster. Storing all images in public cloud is costly. To strike the balance between these two besides preserving privacy and making it computationally efficient, instead of using cryptographic primitives, we prefer segregating sensitive and insensitive data. Sensitive data is very small in quantity while insensitive data is bulky. Therefore insensitive data is sent to public after reducing the data to a text file for storage and computational efficiency. The computationally efficient, secure and privacy preserving data storage on public cloud is illustrated in Figure 2.

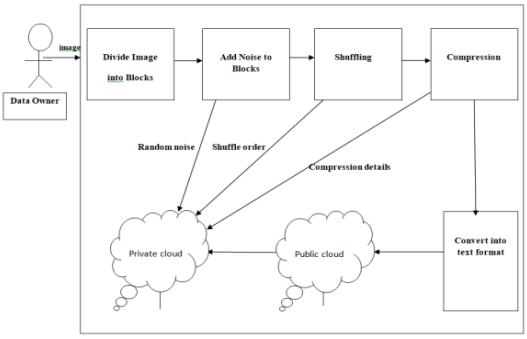


Figure 2: Secure and Privacy Preserving Storage of Image Data on Hybrid Cloud

As illustrated in Figure 2, it is evident that the given image is divided into many blocks of same size. Afterwards, random noise is added to every block by manipulating colour dimensions. After adding noise, the blocks are shuffled to make the image unreadable. The private cloud does not store the whole image information. Instead it stores limited information with which can help user to obtain full information from public cloud. The information stored in private cloud is IMAGE ID, random noise parameter, shuffle order information, and compression information. This information consumes less storage. However, it is known as sensitive information that is very securely stored in private cloud. On the other hand the data stored in public cloud is highly secure and privacy is preserved as adversaries cannot infer any useful content from the data stored in public cloud. After performing shuffling, the shuffled data is subjected to compression which results into compressed image to make transfer of data efficiently. The compressed image data is ultimately converted into a text while which occupies very less space in pubic cloud. The conversion to text is an iterative process in which each pixel, its position and RGB values are written to a file. The final data is stored in public cloud in the form of a text file. This is evident that there is hybrid cloud in which the data stored. It is the wide and efficient segregation of data into sensitive and insensitive data and stored in private and public clouds simultaneously. Therefore, the data is said to have been stored on hybrid cloud. Now in the private cloud, actual image information does not exist. However, it can be used to obtain actual information from public cloud. The data retrieval phenomenon is illustrated in Figure 3. The whole process of retrieving

Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

required image data is boiled down to query processing.

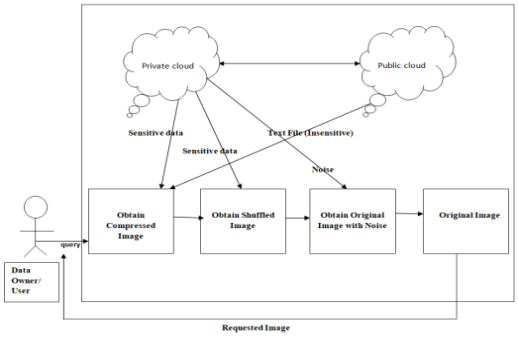


Figure 3: Secure and Privacy Preserving Image Retrieval from Hybrid Cloud

The common information stored on private and public clouds is the ID of image. Therefore, data owner or user needs to provide image ID as input to the system. Image ID is considered to be the query given. Once the query is received, the corresponding data which is in text format needs to be obtained in the form of compressed format. Decompression of such data gives shuffled image. Then the shuffled image is converted to normal image which contains noise introduced. Then the image with noise is subjected to removal of noise to obtain original image. In the process, it is very important to observe that the sensitive data stored in private cloud is utilized. While obtaining compressed image it uses text file related to image from public cloud (insensitive data) and compression information (sensitive data) from private cloud. Later on shuffled image is obtained by using shuffle order (sensitive data) from private cloud. Afterwards, the image with noise is obtained by using noise information (sensitive data) from private cloud. With this the system model is supporting both image storage and retrieval to/from hybrid cloud. The system is thus capable of scaling to large number of images as the private cloud is sensibly utilized.

3.2 Secure Storage Process

Efficiency of image processing is improved if the image is divided into several equal sized blocks. The given image (N x N) is divided into n number of blocks of size k x k. We have taken Lena image with 256 x 256 size and divided it into 3 x 3 sized equal number of blocks. Thus the image is divided into 9 blocks. Therefore the value of n is 9. After converting image into n blocks, each block is subjected to adding noise. Each pixel value in a block is 0 to 255. A random value is taken between 0 and 255. Each pixel value is subtracted from the random value. As different random values are used to add noise to each block, the noise information is stored in private cloud and associates it with image ID. Adding noise is done at block level and the resultant image is blurred. However, the modified image so far is comparable with original image and human eye perception can identify the image. To avoid this identification problem, the image with noise is further subjected to shuffling.

Table 1: RGB Combination for Basic Colours.

Colour	Red	Blue	Green
Black	0	0	0
White	255	255	255
Yellow	255	255	0
Dark Green	0	100	0

The purpose of shuffling is to make the image not understandable. After performing shuffling, the mage is unreadable and thus privacy is preserved. In order to make it more computationally efficient in storing and retrieving and make is more secure, the shuffled image is further subjected to compression and then converted to a text file before storing it in public cloud.

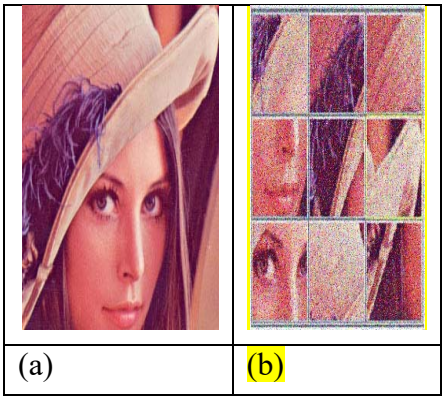


Figure 4: Result of Shuffling (a) Original Image (b) Noised and Shuffled Image

As shown in Figure 4, it is evident that the original image is split into number of blocks and then shuffled with a shuffle order which is saved to private cloud. Shuffling makes the blocks to have improper organization so as to modify the image further. Such image cannot be understood easily.

Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The compression technique is employed after shuffling. It is done based on the mechanism explored in [28] which is known as Harmony Search Algorithm (HSA). This method has three phases namely initialization, harmony improvisation and selection. Before applying HSA, it needs pre-processing which is done as in Eq. 1.

$$\sigma^2=\frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(x_{ij}-\mu)^2}{n} \quad (1)$$

This pre-processing is meant for separating red (R), green (G) and blue (B) parts of given image in order compute variance of each component. Component with least variance is finally selected for compression. Harmony memory is initialized with harmony components from given image. Each element is a 2x2 pixel block from a selected RGB component. Then each element is initialized with value between 0-255. The HSA algorithm optimizes selected RGB and uses it to create compressed image. The algorithm makes use of termination criterion to end optimization process, harmony memory size to determine the number of vectors for solution needed. It also contains information related to the rate at which the intended solutions are obtained from memory. It also has provision for rate of adjusting a value of harmony memory and improvisation of harmony besides choosing the best harmony solution. The quality of produced image after compression can be evaluating using a measurement. It is known as Peak Signal – to – Noise Ratio (PSNR) which is computed as in Eq. 2.

$$\text{PSNR}=10og_{10}\frac{255^2}{MSE} \quad (2)$$

Where Mean Square Error (MSE) is computed as in Eq. 3.

$$\text{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j-K(i,j)]^2 \quad (3)$$

When PSNR is computed for original image and compressed image, it is possible to find whether the image is degraded in its quality. A high PSNR value implies less visual deterioration in the resultant image. PSNR is measured using decibels (dB). The compression information is saved to private cloud. After compression, the image is converted into simple text file and stored in public cloud.

3.3 Secure and Privacy Preserving Image Storage (SPPIS) Algorithm

We defined an algorithm for secure and privacy preserving image storage in hybrid cloud. It makes use of private and public clouds to store sensitive and insensitive information separately and respectively. The given image is stored in public cloud in text file formation after transformation.

Algorithm: Secure and Privacy Preserving Image Storage (SPPIS) Algorithm
Inputs : Image identification *ID*, image *img*, compression quality factor *cqf*, no. of blcoks *m*, amount of noise *na*, strength of noise *sn*, shuffle order *so*
Outputs : ID, so, cqf, noise information (sensitive information) stored in private cloud and text file of *img* stored in public cloud with same ID

Divide Image Into Blocks
1: Compute block size s based on *m*
2: **For** *i*=1 to *m* **Do**
3: b=Divide*Img*(*img*, *s*)
4: Add b to *img'*
5: **End For**
6: *img* = *img'*
7: *img'*=*null*
Adding Noise to Image
8: **For** i=1 to m **Do**
9: b=Noise*Img*(*img*, s)
10: Add b to *img'*
11: **End For**
12: *img* = *img'*
13: *img'*=null
Image Compression and Final Output
14: Compress *img* using Eq. 1 to get *img'*
15: convert *img'* to text file t*img*
16: save *ID*,*so*, *cqf*, *na*, *sn*, and *so* to private cloud
17: save *ID* and *timg* to public cloud
18: return *ID*

Algorithm 1: Secure and Privacy Preserving Image Storage on Hybrid Cloud

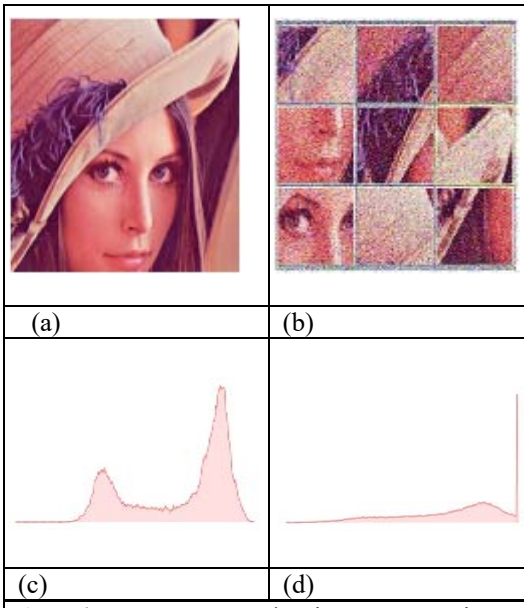
This algorithm is executed by the prototype application that runs in the local machine. However, the information is stored in both private and public clouds. As shown in Figure 2, the sensitive information is stored in private cloud while insensitive and bulky information is stored in public cloud. This approach makes the image content secure and privacy is preserved. Moreover, it is computationally efficient when compared with cryptographic solutions like AES.

3.4 Secure and Privacy Preserving Image Retrieval (SPPIR) Algorithm

Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We defined an algorithm for secure and privacy preserving image retrieval from hybrid cloud. It makes use of private and public clouds to retrieve sensitive and insensitive information respectively. The requested image is retrieved from public cloud in text file formation and then corresponding sensitive details from private cloud for transforming them into original image.



(a) (b)

(c) (d)

Algorithm: Secure and Privacy Preserving Image Retrieval (SPPIR) Algorithm
Inputs : Image identification *ID*
Outputs : Original image
1: Get text file from public cloud
2: Get sensitive info from private cloud
3: Generate a compressed image
4: Uncompress and remove noise
5: Remove explicit blocks
6: Return original image

Algorithm 1: Secure and Privacy Preserving Image Retrieval on Hybrid Cloud

This algorithm is executed by the prototype application that runs in the local machine. However, the information is retrieved from both private and public clouds. As shown in Figure 3, the sensitive information is retrieved from private cloud while insensitive and bulky information is retrieved from public cloud. This approach makes the image content retrieval secure and privacy is preserved. Moreover, it is computationally efficient when compared with cryptographic solutions like AES.

4. EXPERIMENTS AND PERFORMANCE ANALYSIS

We configured local cloud with Aneka [25] cloud platform. Amazon AWS is used as public cloud. A prototype application is built to demonstrate proof of the concept. It is a Swing GUI application built using Java platform. The performance of the proposed system is evaluated using different metrics. Histogram is one of them. Another performance measures used include delay and computational time taken by the proposed algorithm when compared with existing algorithm.

4.1 Histogram Analysis

Histogram is the graphical representation of numerical data. The distribution of numerical data is presented graphically. This can help to understand the subtle difference between two images. Histogram for original image and shuffled image is generated and presented in Figure 4. Histogram shows the difference between original image and changed image with lot of difference. The significant difference or complete difference between the histogram of original image and change imaged for human eye reveals that identifying original image is difficult. Moreover, we further compressed the image and then converted to a text file which does not reflect any details directly of original image. This way the privacy of data is preserved while it enforces secure storage and retrieval in hybrid cloud.

Figure 5: Original image (a), histogram of original image (b), shuffled image (c) and histogram of shuffled image (d)

The original image is subjected to division of blocks, noise and shuffling. Thus the shuffled image cannot help directly to identify original image. Moreover, the shuffled image is subjected to compression and then converting into text file.

```
-----------------------------------------
Image lena colour4
Image Dimension: Height-256, Width-256
Total Pixels: 65536
-----------------------------------------
Pixel (0,0): 255 202 93 99
Pixel (0,1): 255 191 82 88
Pixel (0,2): 255 192 85 91
Pixel (0,3): 255 197 90 96
Pixel (0,4): 255 196 91 96
Pixel (0,5): 255 190 85 90
```

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
Pixel (0,6): 255 187 84 88
Pixel (0,7): 255 204 101 105
...
```

Listing 1: Output File for Lena Image Which is Stored in Public Cloud

As shown in Listing 1, the information presented is related to pixels in the compressed image. It is impossible to get original image from this image. The reason behind this is that its compression information, shuffling information and noise information are in private cloud that is not accessible.

4.2 Overhead Analysis

The proposed system achieves dual goal of data privacy in public cloud and minimizing communication overhead. Considering an image divided into n number of parts and clustered with cluster size as s, the communication overhead of the proposed system with respect to private cloud is computed as in Eq. 4.

$$f(s,t_n) = (t_n \times t_n \times 3) + \left(\frac{t_n}{s} \times 3\right) + H \quad (4)$$

Where H refers to the size of TCP/IP header. Total number of boxes is denoted as tn. Cluster size is denoted as s. The minimization of overhead on the Aneka [25] private cloud built locally is computed as in Eq. 5.

$$Minimize f(s,t_n) = (t_n \times t_n \times 3) + \left(\frac{t_n}{5} \times 3\right) + H$$

$$with\ constaints\ on:$$

$$\frac{t_n^{\frac{t_n}{s}} \times s^{\frac{t_n}{s}} \times \left(\frac{t_n}{s}\right)!}{1000 \times 10^6 \times 60 \times 60 \times 24 \times 365} > 200 \quad (5)$$

and

$$p(DE) = \frac{|DE|}{|\Omega|} < maxi - probability$$

The final pairs that satisfy given constraints can be achieved as in Eq. (6).

$$min - overhead = min\left(f(s,t_n)\right), where 1 \le s \le maximum - s \wedge t_n \ge minimum - t_n \quad (6)$$

4.3 Efficiency Analysis

Our method is efficient in terms of executing time when compared with Advanced Encryption Standard (AES). AES (128 bit key) is a cryptographic algorithm for secure data storage and retrieval. The proposed method and AES are tested in the same environment. Both storage and retrieval operations are performed 100 times and the average execution time is observed. The statistics obtained are presented in Table 2.

Table 2: Execution Time of Proposed Method and that of AES.

Image Size	Execution Time (seconds)		
	Proposed Algorithm	AES	Time Ratio
128*128	0.1317	122.6	931.1
256*256	0.4593	490.1	1067
512*512	1.858	1957	1054
1024*1024	7.01	7.824	1116

Different image size is considered for experiments. The execution time in seconds is presented for proposed method and AES. The difference between them is very huge. It does mean that performance of the proposed method is much higher than that of AES. The difference when image size is 128 x 128 is 931.1 while the time difference is 1116 when image size is 1024 x 1024.

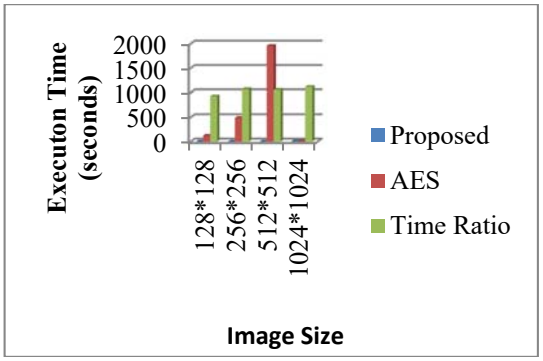


Figure 6: Execution Time Comparison Between Our Method and AES

As shown in Figure 6, it is evident that there are two trends in the results clearly visualized. The first trend is that image size has its influence on the execution time. For instance the execution times for the proposed algorithm when image sizes such as 128 x 128, 256 x 256, 512 x 512, and 1024 x 1024 are 0.1317, 0.4593, 1.858 and 7.010 respectively. It shows clear trend in increasing order proportionately to the size of image. The second trend observed is that the AES algorithm showed more execution time consistently for all sizes of an image. For all block sizes, the proposed method outperformed AES in terms of execution time. The rationale behind this is that the proposed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

solution is not cryptographic and do not have iterations with rounds as AES has. Therefore the propoed method is able to provide data privacy and much faster than cryptographic solutions like AES.

4.4 Delay Comparison with Amazon EC2

Private cloud is built in the local network using Aneka [25] cloud platform. The public cloud consumes resources designated from local network. The public cloud used for the empirical study is Amazon Elastic Compute Cloud (EC2) [26]. Amazon EC2 is a web service which provides secure, resizable and scalable compute resources in pay per use fashion. The sensitive data is stored in MY SQL database stored in private cloud. And the insensitive image data is stored in Amazon RDS which is configured in Amazon cloud. We built a prototype application for storing and retrieving images. The application is built using Java programming language. Swing API is used to have graphical user interface (GUI) while the database connectivity is achieved using JDBC type 4 driver. JDBC driver URL is jdbc:mysql//hostname:port/dbName?user=userName&password=password. The relationship among the proposed application, Amazon EC2 and Amazon RDS is shown in Figure 6.

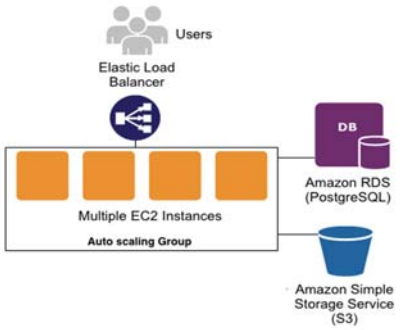


Figure 7: Amazon EC2 Instances With Storage Services [27]

As shown in Figure 7, the users of our application can store image data and retrieve it securely through an Amazon EC2 instance. Amazon EC2 instance is collection of cluster machines that are used to have computations. EC2 instance can have interaction with Amazon RDS and Amazon S3. The illustration provided in Figure 6 is related to public cloud used in this paper. This scenario is true for both storing images and retrieving images with desired level of security and privacy to image data. Experiments are made with the proposed scheme and by passing it without following adding noise, shuffling, compression etc. The overhead when the proposed system is used is negligible as shown in Table 3.

Table 3: Shows Time Delay and Overhead When Proposed Method is Employed

Image Size	With Proposed Method	Without Proposed Method	Delay (%)
128*128	23.3123	22.5023	3.6
256*256	76.1976	73.4673	3.72
512*512	242.4657	230.6346	5.13
1024*1024	976.4206	927.3578	5.29

The results are obtained when the time delay is observed. The difference between the time when server complete processing (t1) and the time at which request is given by end user (t1) is computed as follows. The time measure is milliseconds.

Elapsed time = t2 – t1

Overhead = Elapsed time with proposed system % – Elapsed time without proposed system %.

The results are different for an image with difference sizes. The time delay is increased when the proposed system is used as it needs to communicate with the public cloud that has caused bandwidth overhead. However, the increase in time delay or overhead is almost negligible.

Table 4: Delay Dynamics of Presence And Absence of Proposed Method.

Image Size	Delay (milliseconds)		
	Using Proposed Method	Without Using Proposed Method	Delay Increase (%)
128*128	23.3123	22.5023	3.6
256*256	76.1976	73.4673	3.72
512*512	242.4657	230.6346	5.13
1024*1024	976.4206	927.3578	5.29

As shown in Table 4, the delay is increased when proposed system is used. The minimum overhead is 3.60% for image with size 128 x 128 and maximum overhead is 5.29% for image with 1024 x 1024 size.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

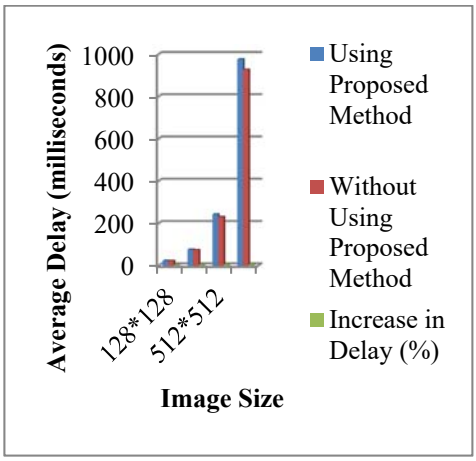


Figure 8: Image Size Vs. Average Delay in Presence And Absence of Proposed Method.

As presented in Figure 8, there are two important observations. The delay time or elapsed time is more as image size is increased gradually. The proposed method consistently exhibited more latency or delay for all image sizes. This is due to the security and privacy preserving mechanisms involved in the proposed methodology. However, it is very encouraging that the delay difference is negligible. This trade off is understandable when security and privacy are guaranteed for outsourced images on hybrid cloud.

5. DISCUSSION

The proposed method is evaluated with images of different size. When compared with the AES standard, the execution time of the proposed method is negligible. In fact the proposed method outperforms AES. Afterward, the delay comparison is made with Amazon EC2, the public cloud environment. Since public cloud is in remote location, there is delay when the proposed method is employed. With 128*128 size the delay is 3.6%, 256*256 3.72 and 1024*1024 it is 5.29. The delay overhead is negligible as trade off between privacy and security and delay. The rationale behind this delay is that the proposed system when connect to public cloud, it has to follow certain standard procedures that cause delay when compared with the local storage. When proposed methodology is used for privacy preserving multimedia content security in public cloud, it provides privacy and security but incurs time delay in the process. As the framework is able to separate given input image into sensitive and insensitive data and outsource insensitive data which is bulky to public cloud. Experimental results showed the efficiency of the proposed method in dealing with computationally efficient storage and retrieval of multimedia content on hybrid cloud.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we studied the problem of data privacy in public cloud. To overcome the increasing concerns about privacy and security of data outsourced to public cloud, we proposed a methodology that addresses these issues. The existing solutions for data privacy and security incurred heavy computational complexity. They also tend to store everything in public cloud. The proposed methodology divides the data of input images into sensitive and insensitive data. Sensitive data is stored in private cloud where the storage cost is not incurred while insensitive data is stored in public cloud. Image ID is used to have correlation between the data stored in hybrid cloud. The given image is divided into number of blocks. Then noise is added to the image so as to make it unreadable. Afterwards, the blocks in the image are shuffled to make more difficult to comprehend the image. Then the image is subjected to compression and ultimately converted to a text file before storing it into public cloud.

In the process, the sensitive data is separated and stored in private cloud. It includes image block information, noise information and compression information that is required while retrieving images from the hybrid cloud. We proposed an algorithm for secure and privacy preserving image storage in public cloud. The reverse process is used in order to retrieve images from hybrid cloud. We built a prototype application to demonstrate proof of the concept. The results revealed that the proposed methodology outperforms existing security algorithms like AES and proves to be computationally efficient besides preserving privacy of image data. It is interesting to investigate and update the methodology for different kinds of data that is outsourced to public cloud. Another direction for future work is to improve the methodology for 2D and 3D videos and videos with multi-view plus depth.

REFERENCES

[1] Niroshinie Fernando Seng W. Loke and Wenny Rahayu. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems. . , p1-33.

[2] Saurabh Kumar Garg , Steve Versteeg and Rajkumar Buyyaa. (2013). A framework for ranking of cloud computing services. Elsevier., p1-12.

[3] Jin Li, Yan Kit , Xiaofeng Chen, Patrick P.C. Lee and Wenjing Lou. (2013). A Hybrid Cloud Approach for Secure Authorized Deduplication. ACM. 26 , p1-12.

[4] Hui Zhang, Guofei Jiang, Kenji Yoshihira, and Haifeng Chen. (2014). Proactive Workload Management in Hybrid Cloud Computing. IEEE. 11 , p1-12.

[5] Ping Lu, Quanying Sun, Kaiyue Wu, and Zuqing Zhu and Senior Member. (2015). Distributed Online Hybrid Cloud Management for Profit-Driven Multimedia Cloud Computing. IEEE. 17 , p1-12.

[6] Ridhi Jindal. (2017). A Review on Recent Development of Image Compression Techniques. JARnD. 1 , p1-7.

[7] Idan Ram, Israel Cohen, Senior Member, and Michael Elad and Fellow. (2014). Facial Image Compression using Patch-Ordering-Based Adaptive Wavelet Transform. IEEE. 21 , p1-5.

[8] Dr. S.Vijayarani1 and A.Sakila. (2016). Document Image Compression using Hybrid Compression Technique. ISSN. 11 , p1-5.

[9] Chuan Qin, Chin-Chen Chang, Fellow, IEEE, and Yi-Ping Chiu. (2014). A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting. IEEE. , p1-11.

[10] Chuan Qin, Chin-Chen Chang, Fellow and Yi-Ping Chiu. (2014). A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting. IEEE. , p1-11.

[11] Zhenjun Tang , Xianquan Zhang and Weiwei Lan. (2015). Efficient image encryption with block shuffling and chaotic map. acm. , p1-21.

[12] M. Monica Subashini, Sarat Kumar Sahoo,Venika Sunil and Sudha Easwaran. (2016). Anon-invasivemethodologyforthegradeidentificationo fastrocytomausingimageprocessingandartificial intelligencetechniques. Elsevier. , p1-12.

[13] Cong Wang, Student Member , Sherman S.-M. Chow, Qian Wang, Student Member, Kui Ren, Member, Wenjing Lou and Member. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE. 62 , p1-12.

[14] Lifei Wei , Haojin Zhu , Zhenfu Cao , Xiaolei Dong , Weiwei Jia , Yunlu Chen , Athanasios V. Vasilakos. (2014). Security and privacy for storage and computation in cloud computing. Elsevier. ., p1-6.

[15] Josef Spillner , Johannes Müller and Alexander Schill. (2013). Creating optimal cloud storage systems. Elsevier., p1-11.

[16] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou. (2015). A Hybrid Cloud Approach for Secure Authorized Deduplication. IEEE. 26, p1-12.

[17] Xueli Huang and Xiaojiang Du (2014) Achieving big data privacy via hybrid cloud. IEEE, p1-7.

[18] Nancy Garg and Kamalinder Kaur2. (2016). Hybrid information security model for cloud storage systems using hybrid data security scheme. IEEE. 3 , p1-3.

[19] MehdiSookhaka,AbdullahGania,MuhammadKhurramKhanb,RajkumarBuyya. (2015). Dynamicremotedataauditingforsecuringbigdata storageincloudcomputing. Elsevier., p1-6.

[20] Chunwang Zhang, Ee-Chien Chang, Roland H.C. Yap. (2014). Tagged-MapReduce: A General Framework for Secure Computing with Mixed-Sensitivity Data on Hybrid Clouds. IEEE, p1-10.

[21] Yong Yua,b, Yafang Zhanga, Jianbing Ni a, Man Ho Auc, Lanxiang Chend, Hongyu Liu. (2014). Improved security of a dynamic remote data possession checking protocol for cloud storage. Elsevier, p1-10.

[22] Xueli Huang and Xiaojiang Du. (2013). Efficiently Secure Data Privacy on Hybrid Cloud. IEEE, p1-5.

[23] Manjrasoft Pty Ltd. (2013). Enabling .NET-based Enterprise Grid and Cloud Computing. Available: http://www.manjrasoft.com/products.html. Last accessed 2017.

[24] Amazon Web Services. (2017). Amazon Elastic Compute Cloud. Available: https://aws.amazon.com/ec2/. Last accessed 2017.

[25] REAL PYTHON. (2015). Deploying a Django App to AWS Elastic Beanstalk. Available: https://realpython.com/blog/python/deploying-a-django-app-to-aws-elastic-beanstalk/. Last accessed 10 June 2017.

[26] Ryan Rey M. Daga and John Paul T. Yusiong (2012). Image Compression Using Harmony Search Algorithm. International Journal of Computer Science, 9(3), p16-23.

[27] Vrunda Jayant Kulkarni, Prof. S.D.Satav and Prof. Darshana Patil. (2016). Survey on Cloud-Based Multimedia Content Protection. International Journal of Engineering Science and Computing. 7 (1), p4004-4007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[28] K.Sai Manoj, Mrudula Kudaravalli and K Phani Srinivas. (2017). A Survey on Protection of Multimedia Content in Cloud Computing. International Journal of Computer Science and Mobile Computing. 6 (11), p7 – 11.

[29] Nikos Fotiou and George Xylomenos. (2016). Protecting medical data stored in public Clouds, P1-6 .

[30] Omar Tayan. (2017). Concepts and Tools for Protecting Sensitive Data in the IT Industry: A Review of Trends, Challenges and Mechanisms for Data-Protection. International Journal of Advanced Computer Science and Applications. 8 (2), p46-52.

`