HS2Cloud: A Secure Lightweight Framework for Image Storage on Hybrid Cloud

Dr.K.Bhargavi [1], M.Kiran Kumar[2], Dr.M.I.Thariq Hussan[3], Dr.D.Stalin Alex[4]

[1]*Associate Professor & Head, Department of Computer Science and Engineering, PVKK Institute of Technology, Anantapur-515001, India.*

[2]*Assistant Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus.*

[3]*Professor & Head, Department of Information Technology, Guru Nanak Institutions Technical Campus,*

[4]*Professor & Head, Department of Information Technology, Guru Nanak Institute of Technology, Hyderabad-501506, India.*

ABSTRACT

Multimedia content providers traditionally used their own facilities to store and manage data. With the emergence of cloud computing that leverages usage of computing resources on-demand in pay per use fashion, the content providers shifted their IT strategy. They found cloud to be promising alternative for storage and retrieval of their content. However, they have security concerns as cloud storage takes place in remote servers that are treated untrusted. Another concern they have is the cost of outsourcing huge amount of data to public cloud as cloud resources are provisioned in pay per use fashion. In the literature it is found that hybrid cloud usage is suitable to achieve both storage security and also minimize expenditure. In this paper, we proposed a secure and lightweight framework known as HS2Cloud for image storage on hybrid cloud. It has an algorithm to separate sensitive data from non-sensitive data of given set of images prior to outsourcing it to public cloud. Sensitive data is under the control of content provider in private cloud. It occupies less storage space. Insensitive data is stored in public cloud thus utilizing the concept of hybrid cloud. Another algorithm is proposed to retrieve data from hybrid cloud by combining both sensitive and insensitive data to obtain original image content. We built a prototype application to demonstrate proof of the concept. The experimental results showed the significance of the proposed framework.

Keywords* – *Cloud computing, image security, hybrid cloud.

1. INTRODUCTION

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 security concern on outsourced content to cloud. Outsourcing multimedia content to public cloud provides many benefits. One important benefit is affordable storage provisioned to be scalable and available in pay per use fashion.

Multimedia content providers outsource their image data to public cloud. They found two important issues with this. The first issue is security concern as their private data is stored in public cloud on which they do not have control. It does mean that storage of data is taken place in remote servers. The second issue is that, the storage of multimedia content on public cloud incurs more cost. The cost can be reduced and image content can be securely stored in public cloud by considering hybrid cloud approach. Hybrid is the combination of private cloud and public cloud. Therefore it facilitates storage of sensitive data in private

cloud while insensitive and bulky data is outsourced to public cloud.

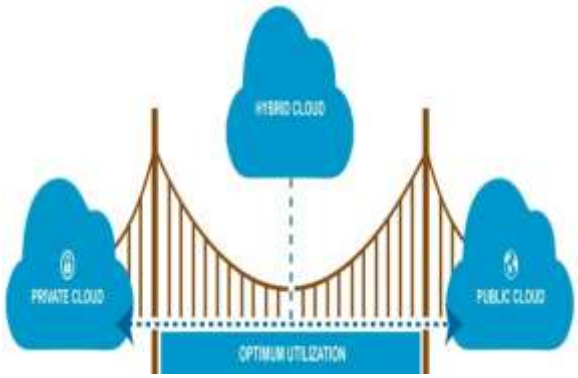

Figure 1: Illustrates the utility of public cloud

As presented in Figure1, the combination of private and public clouds is known as hybrid cloud. It provides the convenience, in-premise storage and security of private cloud and benefits of public cloud that provides unlimited access to computing resources on-demand with scalability and 100% availability. In the literature many hybrid cloud usage is found in [17] where the multimedia content is segregated into two parts before outsourcing it to public cloud. The two parts are nothing but sensitive data and insensitive data. Inspired by the concept, in this paper, we proposed a secure light weight framework which takes care of content segregation and storage and retrieval on hybrid cloud. Local cloud is implemented using Aneka [24] while the public cloud used is Amazon Web Service (AWS) cloud where Amazon Elastic Compute Cloud (EC2) instance is used for public cloud. On top of EC2, Amazon Simple Storage Service (S3) is used for storing insensitive content of images. Our contributions are as follows.

We proposed a secure lightweight framework known as HS2Cloud for provisioning segregation of image content provided by content owner and store it in hybrid cloud. The sensitive content is stored in local Aneka cloud (private cloud) while insensitive data which is more in volume is outsourced to Amazon EC2.

We proposed two algorithms for achieving the intended storage and retrieval of images on hybrid cloud. The first algorithm takes care of content segregation and storage in hybrid cloud while the second one takes care of secure retrieval of images that are constructed by combining content saved in private and public clouds.

We built a prototype application to demonstrate proof of the concept. The application facilitates the configurations related to private and public clouds besides allowing secure storage and retrieval of images as per the functionality of the proposed algorithms. The prototype is evaluated and found to be very useful to content providers who want efficiency, security and minimize cost of outsourcing to public cloud.

The remainder of the paper is structured as follows. Section 2 provides review of literature. Section 3 presents the proposed framework. Section 4 presents experimental results. Section 5 concludes the paper besides providing directions for future work in the area of multimedia content security in cloud.

2. RELATED WORK

This section provides review of literature on cloud security and the means of securing images in cloud. A symmetric encryption scheme is proposed in [1] for sure storage of images. It was found to be effective to defend cryptanalytic attacks. A hierarchical image authentication framework is proposed in [2] for overcoming Vector Quantization (VQ) attacks. Importantly in [3] security defects related to image encryption schemes are explored. It is found that known plain-text attacks were possible on recently proposed chaos-based encryption scheme. A novel image encryption method is proposed in [4] to overcome security limitations of Bit

Recirculation Image Encryption (BRIE). A new 1-D chaotic system is employed for securing images with encryption in [5]. It was tested with various attack and found to be effective.

SecCloud is proposed in [6] for privacy preserving and secure cloud storage. It performs storage and computations auditing. A thorough security analysis is made on the cryptosystems in [7] for finding vulnerabilities. Cloud based multimedia content protection system is proposed in [8] for protecting multimedia content in public cloud. Traffic security architecture for protecting multimedia content is proposed in [9] while protecting images with different kinds of encryption techniques is explored in [10]. A video copy detection system to prevent privacy of multimedia is the focus in [11]. Multimedia content protection is explored in [12] which are similar to that of [8], [18] and [21]. Security and privacy issues in public cloud are studied in [13]. They found issues like data sharing, access control, complexity, protection of interests of parties, legal compliance and intrusion detection. Security optimizations for cloud services are provided in [14]. With respect to big data stored in cloud, the data privacy and security with regard to security expectations is the main focus in [15].

Select region protection for surveillance videos in cloud is the study made in [16]. Cloud data privacy and security in hybrid cloud is the important research made in [17] which is somewhat close to our work in this paper. Various multimedia content protection systems associated with cloud are reviewed in [19] while concepts and tools that can be used to protect sensitive data are studied in [20]. Security threats in cloud are categorized in [22]. Data and image security mechanism is proposed in [23]. As found in the literature the paper [17] has triggered the work in this paper. The proposal of a framework for securing images with a hybrid cloud and reducing the cost of using public cloud is the important study made in this paper.

3. PROPOSED FRAMEWORK

We proposed a framework known as HS2Cloud for secure and light weight storage and retrieval of images on hybrid cloud. The framework makes use of both private and public clouds in order to optimize security and reduce cost of outsourcing to public cloud. This framework is intended to help multimedia content owners to have secure storage of images and secure retrieval of the same on hybrid cloud. Private cloud is built using Aneka [24] while the public cloud used is Amazon EC2 [25]. The rationale behind the usage of Aneka is that it is simple cloud platform based on Microsoft .NET platform. Its implementation in the local computing resources is easier. The reason behind AWS cloud is that its EC2 and S3 are widely used to outsource data as the public cloud has its presence in all regions of the world. Content owner interacts with the framework to store images and retrieve them. The phenomenon of storage and retrieval are different as the framework achieves dual benefits such as security and reducing cost of public cloud usage.

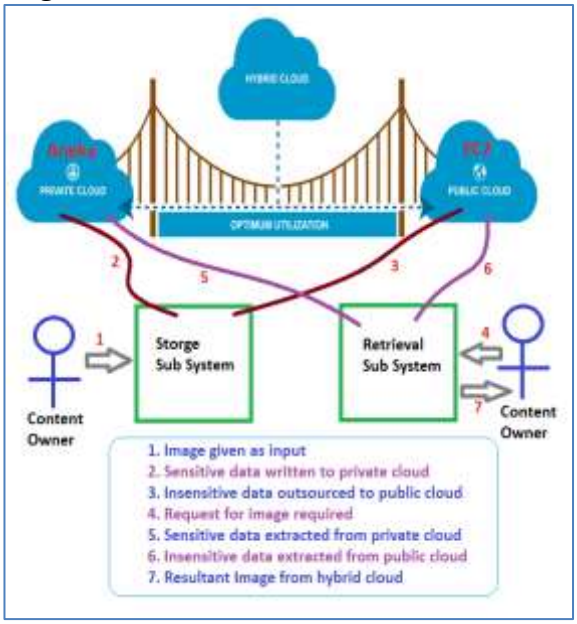

Figure 2: Overview of the proposed framework HS2Cloud

As presented in Figure 2, it is evident that the proposed framework has two subsystems. The first sub system is meant for storage while the second one is meant for retrieval of images. The flow of the framework is as follows.

1. Content owner chooses image (s) to be stored in hybrid cloud.
2. The storage sub system segregates given image (s) into two parts. Sensitive data and insensitive data are segregated before storage.
3. Sensitive data is stored in private cloud.
4. Insensitive data is stored in public cloud.
5. Content owner makes request for image (s).
6. The retrieval sub system of the framework gets related sensitive data from private cloud and insensitive data from public cloud and generates requested image (s).
7. Then the content owner gets requested image (s).

3.1. Storage Sub System of HS2Cloud

The proposed framework is thus able to provide secure cloud storage and retrieval besides gaining advantages of reducing cost of public cloud usage. The framework is further elaborated by giving more details of storage and retrieval sub systems respectively. The storage sub system is illustrated as in Figure 2 while the retrieval sub system is illustrated as in Figure 3.

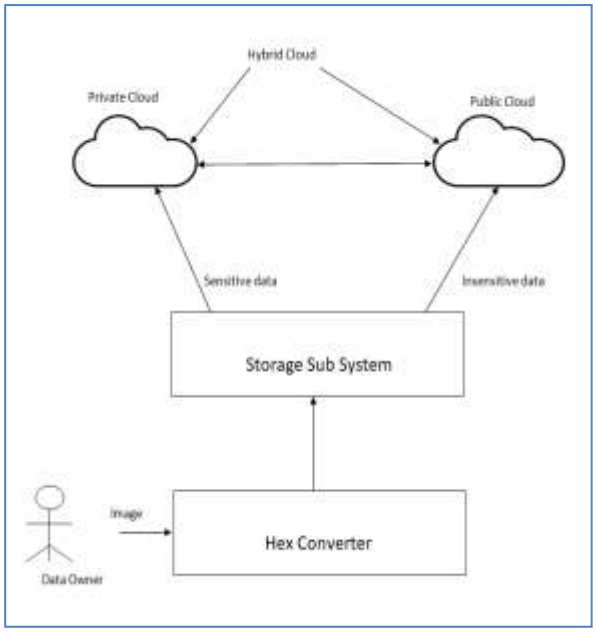

Figure 3: Overview of the storage sub system of HS2Cloud

As shown in Figure 3, the given image by the content owner is subjected to hexa decimal conversion. Then the converted data is segregated into sensitive and insensitive data before storing in hybrid cloud. The sensitive data quantity is very less. Therefore it is stored in private cloud. It contains image identity and summary of image besides conversion details that can be used to reconstruct image. Insensitive data is bulky and it is stored in public cloud. Once data is stored in public cloud, the content owner is notified about it and such data can be retrieved again.

3.2 Secure Image Hybrid Cloud Storage (SIHCS) Algorithm

Algorithm: Secure Image Hybrid Cloud Storage

Input : Images ***I***

Output: Secured and saved image content on hybrid cloud

01 Initialize image parameters vector P
02 Initialize image'
03 For each image in I
04 P = ExtractParams(image)
05 Add transformation parameters to P
06 image'=Transform(image)
07 Save P to private cloud
08 Save image' to public cloud
09 End For

Algorithm 1: Secure image hybrid cloud storage algorithm

The algorithm takes set of images as input and follows the methodology of storage sub system. It takes an image and then extracts its parameters and transformation parameters that can be used later for reconstruction of image. The parameters (sensitive data) are stored in private cloud. Then the transformed image that is converted hexa decimal and some additional transformation information for security is saved to public cloud.

3.3 Retrieval Sub System

The retrieval sub system is part of the proposed H2SCloud framework. It makes use of given image as query and obtains its related information from private and public clouds. Then it reconstructs the original image.

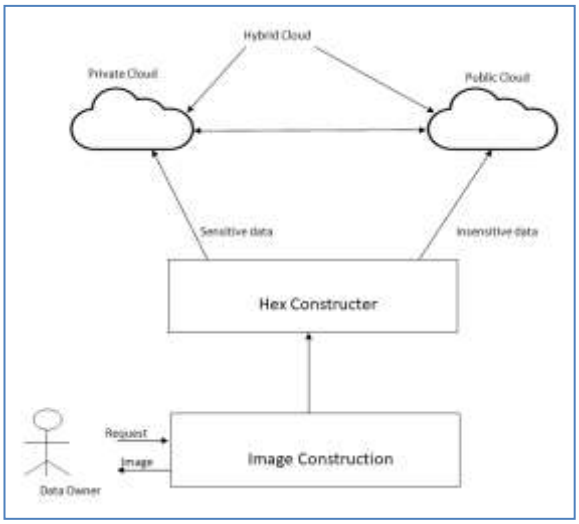

Figure 4: Overview of retrieval sub system of HS2Cloud

As presented in Figure 4, it is evident that the retrieval sub system allows content owner to make queries. When a query is made for an image, the request is processed by the sub system. It takes corresponding sensitive data from private cloud. With the information in the private cloud, the corresponding image content (insensitive data) is taken from public cloud. Then the Hex Constructor constructs whole image content which is finally subjected to construction of original image. The resultant image is provided to content owner who made the request for image.

3.4 Secure Image Retrieval (SIR) Algorithm

Algorithm: Secure Image Retrieval

Input : image *id*

Output: Reconstructed image

01 Initialize image parameters

vector P
02 Initialize image
03 Initialize image'
04 P = ExtractParameters(*id*)
05 image = ExtractInsensitiveInfo(*id*)
06 image'=ReconstructImage(P, image)
07 Return image'

Algorithm 2: Secure image retrieval algorithm

The algorithm takes an image id or request for an image as input and returns the requested image. Once the request is made, the algorithm extracts its parameters from private cloud and its insensitive information from public cloud. Then the algorithm reconstructs the image and returns it to the content provider.

4. EXPERIMENTAL SETUP

Experimental setup is made with two clouds. Private cloud is built using Aneka [24] cloud platform while the public cloud considered is EC2 [25]. Aneka is from Manjra soft company while EC2 from Amazon. EC2 is web services based cloud platform that provides scalable, available services in terms of computing resources provisioned in pay per use fashion. Amazon S3 is used for storage which runs on top of EC2. Amazon cloud storage services are illustrated as in Figure 4. There are two storage services such as S3 (for unstructured and semi-structured data) and Amazon Relational Data Service (RDS) for structured or relational data.

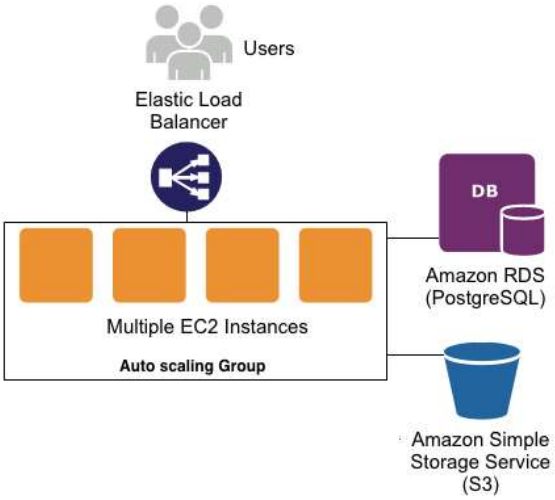

Figure5 : Amazon EC2 instances with storage services

As shown in Figure 5, it is evident that it is possible to access AWS cloud by using Amazon EC2. Once EC2 cluster instance is created, it facilitates the configuration of S3 and RDS. Once they are configured, they provide the URL through which programming languages like Java can access the web services of Amazon for handling storage and retrieval.

5. EXPERIMENTAL RESULTS AND EVALUATION

This section provides the details of experiments made, the results observed and evaluation of the proposed framework HS2Cloud.

5.1. Input Files Used from Medical Dataset

Medical dataset is collected from Internet sources. However, the framework works for any kind of image storage. As the medical images are related to healthcare domain, they are used for experiments. The rationale behind this is that healthcare industry produces multimedia content especially images that is to be protected and used as and when required. This industry can save the public cloud storage by configuring a hybrid cloud setup.

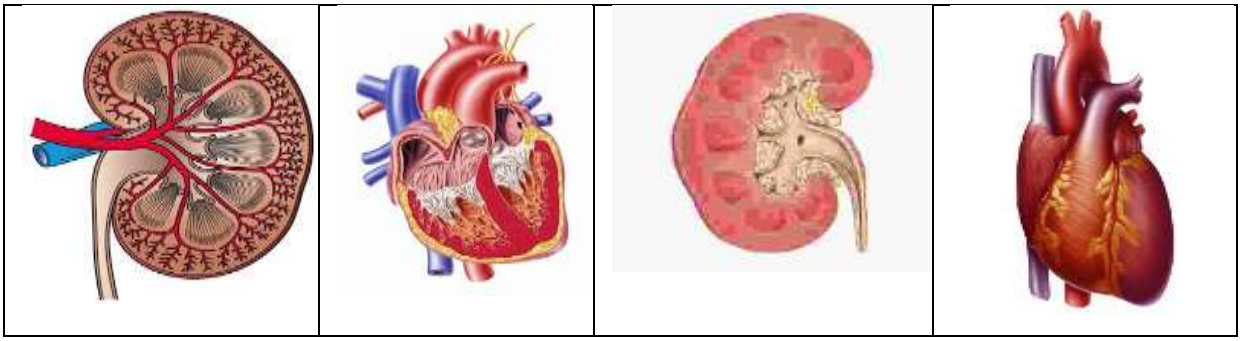

Figure 6: Shows input images

As shown in Figure 6, an excerpt of medical images considered for experiments. These images are used with our prototype application built using Java programming language. The interface is built using Swing while the AWS API is used to connect to public cloud. When an input image is given to the framework, it converts the image into hexa decimal file. Then the hexa decimal content is subjected to transformation and the transformation information and image identity are stored in private cloud while the actual image content which is in converted format is stored in public cloud. Listing 1 shows an excerpt of the hexa decimal content produced for given image.

```
0x41, 0xDC, 0x11, 0xB8, 0x22, 0xC6, 0x00,
0xE5, 0x5D, 0xA1, 0xEC, 0x16, 0x67, 0x28,
0xC6, 0x5C, 0xA9, 0x69, 0xA3, 0xF2, 0x14,
0x65, 0x51, 0xE4, 0xCB, 0xCA, 0x65,
0x1B, 0xEE, 0x3C, 0x7E, 0x84, 0xDB,
0x63, 0x29, 0xD9, 0x29, 0x1D, 0xF6, 0x5B,
0x5D, 0x70, 0xB4, 0xF3, 0xFB, 0xAD,
0xE6, 0x5A, 0x6C, 0xE2, 0x4F, 0xA5, 0x66,
0x07, 0x4A, 0x31, 0xD4, 0x14, 0x12, 0x0B,
0x51, 0x50, 0x1D, 0x7D,
…
…
0x00, 0xC0, 0x06, 0x00, 0x30, 0x01, 0x80,
0x0C, 0x00, 0x60, 0x03, 0x00, 0x18, 0x00,
0xC0, 0x06, 0x00, 0x30, 0x01, 0x80, 0x0C,
0x00, 0x60, 0x03, 0x00, 0x18, 0x00, 0xC0,
0x06, 0x00, 0x30, 0x01, 0x80, 0x0C, 0x00,
0x60, 0x03, 0x00, 0x18, 0x00, 0xC0, 0x06,
0x00, 0x30, 0x01, 0x80, 0x0C, 0x00, 0x60,
0x03, 0x00, 0x7F, 0xFF, 0xD9,
```

Listing 1: Expert from output of image 1

Then the hexa decimal content is transformed and stored in public cloud while the sensitive information that can identify image and help in reconstruction is stored in private cloud.

5.2. Results and Evaluation

Execution time and time delay are the measures used to evaluate the proposed system besides the ability to secure image content efficiently on hybrid cloud. The performance of the proposed framework is

compared with that of AES encryption used to secure images.

Table 1: Execution time performance

Image	Execution Time (seconds)	
	Proposed framework	**AES**
1	0.0128	65.6
2	0.0321	67.3
3	0.0215	64.8
4	1.0354	66.2

As presented in Table 1, it is evident that the results of four images in terms of execution time for all chosen images. The proposed framework shows superior performance over AES algorithm.

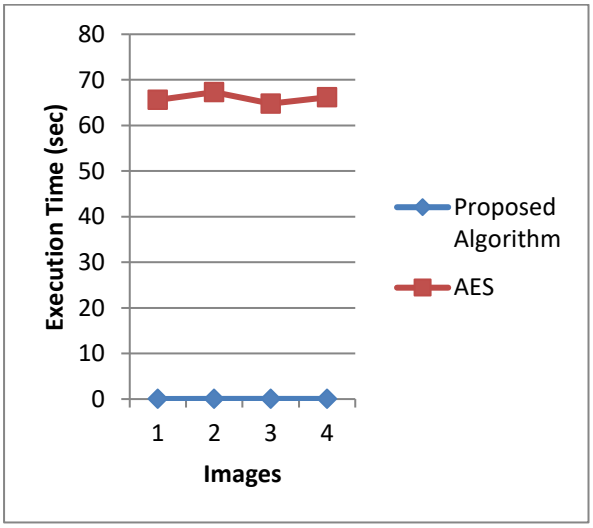

Figure 7: Execution time comparison

As presented in Figure 7 it is evident that the images are shown in horizontal axis while the execution time in seconds is shown in vertical axis. The proposed framework showed negligible time taken for the secure storage of images while the encryption done using AES for image security took long time.

Table 2: Delay time comparison

Image	Delay Time (milliseconds)	
	With Proposed Method	Without Proposed Method
1	10.3165	9.3242
2	10.1976	9.3654
3	10.4657	9.5462
4	10.4206	9.3273

As shown in Table 2, it is evident that the proposed framework showed relatively more time as it needs to consider segregation of image content and then transforming and storing in public cloud. Therefore the delay time of the proposed system is slightly more than that of the system that does not use the proposed framework. The overhead on the proposed system is negligible as it provides secure image storage and retrieval on public cloud besides reducing cost of public cloud usage.

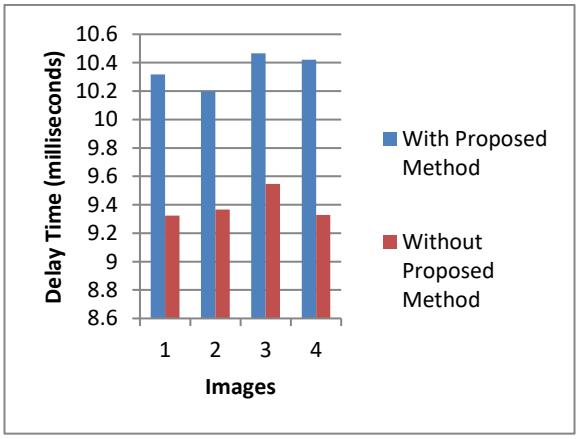

Figure 8: Delay time performance comparison

As presented in Figure 8, it is evident that the images used for experiments are taken in horizontal axis while the vertical axis

represents the delay time in milliseconds. The results revealed the observations on a system for storing images in public cloud with and without using the proposed framework. When the proposed framework is not used, it is bit faster as it does not incur the burden of content segregation and transformation process. Though the proposed system causes more delay, it is negligible and the security and storage benefits it bestows outweigh the delay cost.

Table 3: Delay time comparison

Image	Delay Time (milliseconds)	
	Direct Compressed Image	With Proposed Method
1	9.8978	10.2354
2	9.6756	10.3686
3	9.4579	10.9856
4	9.3452	10.2654

As shown in Table 3, it is evident that the proposed framework showed relatively more time as it needs to consider segregation of image content and then transforming and storing in public cloud. Therefore the delay time of the proposed system is slightly more than that of the system that does not use the proposed framework and use compressed images directly. The compression is made using the technique explored in [26]. The overhead on the proposed system is negligible as it provides secure image storage and retrieval on public cloud besides reducing cost of public cloud usage.

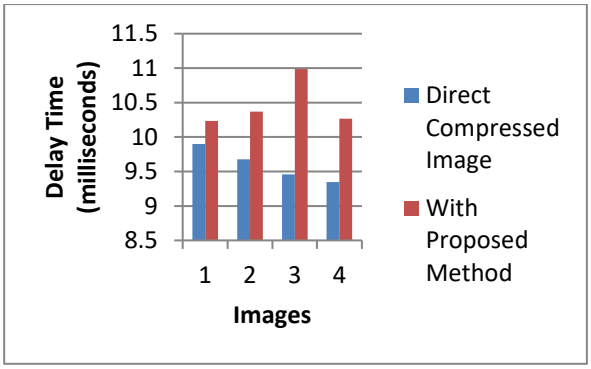

Figure 9: Delay time performance comparison with direct compressed images

As presented in Figure 8, it is evident that the images used for experiments are taken in horizontal axis while the vertical axis represents the delay time in milliseconds. The results revealed the observations on a system for storing images in public cloud with and without using the proposed framework. When the proposed framework is not used (direct compressed images are used), it is bit faster as it does not incur the burden of content segregation and transformation process. Though the proposed system causes more delay, it is negligible and the security and storage benefits it bestows outweigh the delay cost.

6. CONCLUSIONS AND FUTURE WORK

In this paper we investigate on the secure image storage on hybrid cloud. Hybrid cloud is the cloud which combines both private and public clouds. Private cloud is under the control of data owner and therefore it is secure cloud. However, public cloud is not considered secured as the data is stored in

remote servers on which the content owner has no control. We considered the case of multimedia content providers. Of late they shifted their IT strategy from traditional storage to cloud storage and retrieval. When they store whole data in public cloud, it costs more. When they store whole data in private cloud, the private cloud gets exhausted. In this paper we proposed a framework that facilitates storage of images in hybrid cloud with security and also provision to reduce the cost of public cloud.

The proposed lightweight framework is known as H2SCloud. It has two sub systems namely storage sub system and retrieval sub system. The former is used to divide the given image into sensitive and insensitive data and store in private and public cloud respectively. The latter on the other hand takes request for image from content owner and gets the sensitive data from private cloud and insensitive data from public cloud and construct the requested image.

We built a prototype application to demonstrate proof of the concept. The experimental results revealed the utility of the proposed framework. In future we intend to improve our framework to support other media files like audio and video.

REFERENCES

[1] *Kai Wang , Wenjiang Pei , Liuhua Zou , Aiguo Song , Zhenya Hea. (2005). On the security of 3D Cat map based symmetric image encryption scheme. Physics Letters, p.432–439.*

[2] Mehmet U. Celik , Gaurav Sharma, Eli Saber, A. Murat Tekalp. (2001). A HIERARCHICAL IMAGE AUTHENTICATIONWATERMARK WITH IMPROVED LOCALIZATION AND SECURITY. Proceedings IEEE International Conference on Image Processing, P.12-19.

[3] Chengqing Li , Shujun Li , Muhammad Asim , Juana Nunez , Gonzalo Alvarez and Guanrong Chen. (2009). On the security defects of an image encryption scheme. Preprint submitted to Image and Vision Computing, P.25-35.

[4] Shujun Li and Xuan Zheng. (2002). On the Security of an Image Encryption Method. Institute of Image Processing, School of Electronics and Information Engineering, p.9001-1110.

[5] Yicong Zhou, Long Bao, C. L. Philip Chen. (2014). A New 1D Chaotic System for Image Encryption. Future Generation Computer Systems, p.21-30.

[6] Lifei Wei , Haojin Zhu a, Zhenfu Cao , Xiaolei Dong , Weiwei Jia , Yunlu Chen , Athanasios V. Vasilakos. (2014). Security and privacy for storage and computation in cloud computing. Information Sciences. 258, p.345-445.

[7] Houcemeddine Hermassi ∗, Rhouma Rhouma, Safya Belghith. (2012). Security analysis of image cryptosystems only or partially based on a chaotic permutation. Preprint submitted to The journal of systems and software, p.23-33.

[8] Mohamed Hefeeda , Tarek ElGamal , Kiana Calagari, and Ahmed Abdelsadek. (2015). Cloud-Based Multimedia Content Protection System. IEEE TRANSACTIONS ON MULTIMEDIA. 17 (3), p.90-102.

[9] Liang Zhou, Nanjng. (2011). Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network, P.30-44.

[10] Zafar Shahid, Marc Chaumont, William Puech. (2011). Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P Frames. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, p.90-102.

[11] Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward. (2011). A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. 6 (1), P.25-35.

[12] Chaya MPP, Dr. K Thippeswamy. (2016). A Secure System for Multimedia Content Protection on Cloud. Future Generation Computer Systems. 3 (7), P.12-19.

[13] Allan Cook, Michael Robinson, Mohamed Amine Ferrag, Leandros A. Maglaras, Ying He, Kevin Jones and Helge Janicke. (2018). Internet of Cloud: Security and Privacy Issues. Future Generation Computer Systems, p.230-330.

[14] Varun M. Deshpande, Mydhili K. Nair and Ayush Bihani. (2018). Optimization of Security as an Enabler for Cloud Services and Applications. Springer, p.23-33.

[15] Elisa Bertino and Elena Ferrari. (2018). Big Data Security and Privacy. Springer, P.12-19.

[16] Xiaojing Ma, Laurence T. Yang, Yang Xiang, Deqing Zou and and Hai Jin. (2015). Fully Reversible Privacy Region Protection for Cloud Video Surveillance. IEEE, p.230-330.

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

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

[19] 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.

[20] 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.

[21] 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.

[22] Tariqul Islam and D. Manivannan. (2016). A Classification and Characterization of Security Threats in Cloud Computing, p1-21.

[23] Tamilarasi R, Prabu S and Swarnalatha P. (2015). An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication (CSA) Protocol Suite. MAGNT Research Report. 3 (8), p133-141.

[24] Christian VECCHIOLA , Xingchen CHUa, and Rajkumar BUYYAa. Aneka: A Software Platform for .NET-based Cloud Computing, P1-30.

[25] Gurudatt Kulkarni, Ramesh Sutar Jayant Gambhir . (2012). "CLOUD COMPUTING-INFRASTRUCTURE AS SERVICEAMAZON EC2.International Journal of Engineering Research and Applications. 2 (1), p117-125.

[26] T. Bhaskara Reddy , Hema Suresh Yaragunti , T. Sri Harish Reddy and S. Kiran. (2014). An Efficient Approach for Image Compression using Segmented Probabilistic Encoding with Shanon Fano[SPES]. International Journal of Computer Science Engineering and Technology(IJCSET). 4 (6), p200-207.