ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Two Dimensional Image Scaling and Cropping in Secure Data Sharing Cloud Environment

Jadhav Rohini, B. S. Kurhe

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, India

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, India

ABSTRACT: The progression of cloud computing and a radical augmentation in image size are making the outsourcing of image storage what's all the more, taking care of an engaging business appear. Regardless of the way this outsourcing has numerous central focuses, ensuring data arrangement in the cloud is one of the key concerns. There are state-ofthe-craftsmanship encryption gets ready for ensuring arrangement in the cloud. In any case, such plans don't allow cloud datacenters to perform operations over encrypted images. This framework, address this stress by proposing 2DCrypt, a balanced Paillier cryptosystem-based image scaling and cropping arrangement for multi-client settings that grants cloud datacenters to scale and alter an image in the encrypted space. To expect a high storage overhead occurred on account of the honest per-pixel encryption, we propose a space-capable tiling arrangement that grants tile-level image scaling and cropping operations. In a general sense, as opposed to scrambling each pixel independently, we can encode a tile of pixels. 2DCrypt is with the true objective that different clients can view or process the images without sharing any encryption keys – an essential appealing for useful game plans in certifiable affiliations. Our examination and results show that 2DCrypt is IND-CPA secure and realizes a sufficient overhead.When scaling a 512 x 512 image by a segment of two, 2DCrypt requires an image client to download about 5:3 conditions a bigger number of data than the un-encrypted scaling what's more, need to work around 2:3 seconds more to get the scaled image in plaintext.

KEYWORDS: Key,Encryption,Fine grained,Access Control

I. INTRODUCTION

The measure of advanced images has detonated lately dueto the multiplication of computerized imaging gadgets with expanding determination. People and associations are starting torely on outsider datacenters (e.g., cloud datacenters or data-focuses of interpersonal organization specialist co-ops) to store, process,share, and oversee images.As these images could be exceedingly individual and could contain sensitive information (e.g., MRI output of a patient), this pattern has prompt worries about image secrecy andimage uprightness. Initially, a foe who can accessthe image put away at a datacenter can acquire possibly sensitive information contained in an image, prompting privacyloss. Also, a foe may change the image put away ata datacenter to give deceiving information. Therefore,datacenter-based image storage frameworks must organize theneed to secure the image in the datacenters.To ensure image classification and respectability, one can usesecret image sharing [3] to conceal an image (i.e., the mystery image) from any of the datacenter by appropriating the shares(i.e., the shadow images) over various datacenters. Existing recommendations for mystery image sharing, especially, thosebased on Shamir's mystery sharing plan and multi-mystery image sharing plans, fundamentally concentrate on the tradeoff betweenefficiency and security, and don't effectively bolster image operations on the shadow images.Two essential image operations on expansive images are scaling and cropping.

Downloading a substantial image, for example, ahistopathological image (whose size can be in the request oftens of GBs) to users may not be constantly doable. Users maywant to review a downsized adaptation of the image beforedeciding whether to download the image. Facilitate, users mayjust need see a specific region of enthusiasm for the image, inwhich case, an edited region ought to be downloaded. Thesetwo operations, scaling and cropping, can be

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

joined tosupport zooming and panning, two regular client interactionsto investigate substantial images.Supporting scaling and cropping with mystery image sharing is non-minor. A guileless arrangement would be for the datasource to make various mystery images at various resolutions(to bolster scaling) and to isolate every mystery image into autonomously decodable tiles (to bolster cropping). These tilesare then mystery shared over the datacenters. At the point when users ask for a region of an image at a specific scale, each datacenter sends the shadow tiles that cover with the region at the nearest determination to the client. Such an answer, be that as it may, maycause extra data to be sent to the client. The development of cloud storage and computing stages licenses users to source storage and calculations on their information, and grants organizations to dump the undertaking of keeping up data-focuses. In any case, issues over loss of privacy and business estimation of individual information are an astounding obstruction to the appropriation of cloud services by clients and organizations alike. Great on account of mitigate these privacy issues is to store all information inside the cloud encrypted, and perform calculations on encrypted information. To the present complete, need a cryptography plan that empowers important calculation on encrypted information, especially a homomorphic cryptography conspire.

II. RELATED WORK

The utilization of cryptosystems for concealing images is a very much examined territory. Various methodologies, including yet are not restricted to, Public Key Cryptosystem (PKC) [7], watermarking [8], Shamir's secret sharing [6] and mayhem based encryption, have been proposed to ensure images. These plans give secrecy for cloud-based storage systems where a cloud datacenter does not play out any operation on the put away image. To permit cloud datacenters to perform operations on the encrypted image, halfway homomorphic cryptosystem-based arrangements have been proposed . A halfway homomorphic cryptosystem solely offers either expansion or multiplication operations. Paillier , Goldwasser-Micali Benaloh , Shamir's secret sharing [3] are among halfway homomorphic cryptosystems that bolster expansion. While, cases of halfway homomorphic yptosystems that offer multiplication are RSA and ElGamal . Along these lines, the decision of a halfway homomorphic plan is vigorously reliant on the sort of operations to be performed in the encrypted space. Early works have concentrated on recovering encrypted content records. For example, displayed the primary pragmatic conspire for single keyword inquiry on encrypted records. To enhance execution, broadened the encrypted seek with ordering capacity. Both works have been stretched out for looking utilizing conjunctions of multiple keywords. More late works have concentrated on SQL-like questions supporting conjunctions and disjunctions [2]. Encrypted content based pursuit can likewise be connected to recovery of encrypted images. In any case, the exactness of the returned set is reliant on the nature of the keywords utilized for portraying the substance of an image. Few works have been proposed for looking encrypted images in light of element extraction of image highlights. Lu et al. proposed down to earth seek in light of highlight/record randomization methods that offer a great exchange off between protection safeguarding and execution. proposed a homomorphic-based SIFT (Scale-Invariant Highlight Transform) extraction seek that expands the exactness of the inquiry additionally acquires from 2 to 4 requests of IEEE Transactions on Information Forensics and Security (Volume:PP , Issue: 99),24 June 2016 size more expenses. A later work by [1] presents a look plot for encrypted images that is exact and in the meantime brings about computational overheads like a plaintext strategy. Be that as it may, their plan obliges users to share the keys for getting to images. A few works have been proposed for protection saving confront acknowledgment where one gathering tries to coordinate a confront image with a dataset facilitated by another get-together and both gatherings are keen on keeping their data secret from each other. Shamir's secret sharing has been utilized for permitting encrypted space scaling and cropping [4], [5]. Shamir's secret sharing-based plans, onetheless, can be infeasible for useful situations since they require n cloud servers. Additionally, these plans are inclined to agreement attack when k cloud servers plot. Conversely, 2DCrypt utilizes the Paillier-based cryptosystem that requires just a single cloud datacenter and is more powerful to agreement attacks. The Paillier cryptosystem is homomorphic to increments and scalar multiplications [3] and can be changed to an intermediary encryption conspire.

III. PROPOSED SYSTEM

The proposed system consist of distributed cloud storage.The cloud scale ,crop and encrypt the images on behalf of image outsourcer.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

1.Image Outsourcer
Image outsourcer is hospital authority who stores the image on cloud.The image outsourcer maintains the security and privacy of a particular image.This is obtained by encryption of an image before uploading.Image outsourcer can delete modify images also manage access control policies.
2. Cloud server
Amazon EC2 used as a cloud server for storing and processing the images.Both encrypted images and policies are stored on cloud.
3. Image User
Image user are authorized user by image outsourcer , these user can request images stored on cloud.Authorised user do not need to share any key.Other user can decrypt the image on request approval.
4. Key Management Authority
It generate key pair one for client and one for server.These keys get securely shared via email.

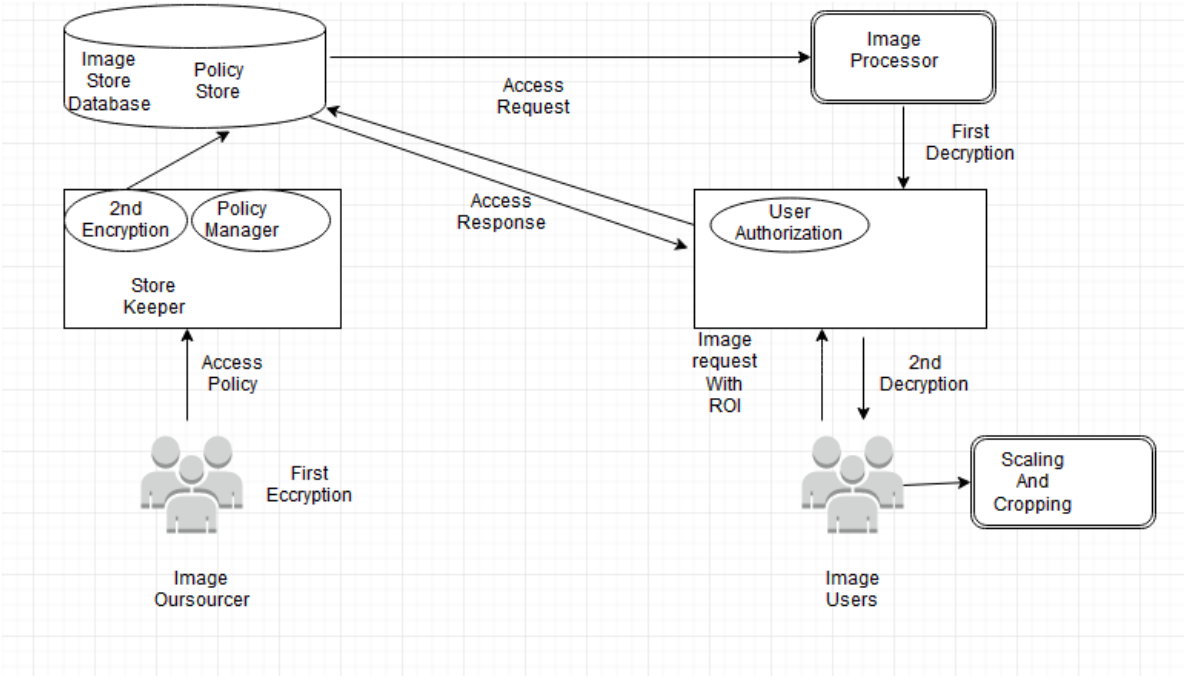

Fig: System Architecture

The Image Outsourcer stores an image and its get to arrangements in the cloud server. For this occupation, the Image Outsourcer invokes its customer module Store Requester by giving plaintext image and get to strategies as data sources (Step i). The Store Requester plays out the first round of encryption on the information image, using the client side key, and after that sends the encrypted image nearby its get to arrangements to the Store Keeper module of the Cloud Server (Step ii). Observe that while scrambling the image, the Store Keeper segments the image into various tiles and performs per-tile encryption. An organized examination about the tile-level encryption will be displayed in Section V. The encrypted image, which is gotten by the Cloud Server, is not in the normal course of action essential for partaking in multi-client settings. At the Cloud Server-end, the Store Keeper plays out the second round of encryption using the server-side key identifying with the client, and stores the encrypted image in an image store (Step iii.a). The Store Keeper in like manner stores the get to arrangements of the image in the Policy Store (Step iii.b). Once an Image User envisions that the Cloud Server will set up any image, its customer module Access Requester gets its info (Step 1). The module Access Requester surveys the scaling and cropping parameters and advances the demand to the Access Request Processor module of the Cloud Server (Step 2). In the demand, the Access Requester sends image scaling/cropping

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

parameters, (for instance, scaling component and in addition cropping ROI) and client certification (which can be anonymized) to the Access Request Processor. The Access Request Processor in any case plays out a client endorsement arrange by sending a get to demand to the Access Manager (Step 3). The Access Manager brings the get to approaches for the asking for client from the Policy Store (Step 4) and it arranges the get to strategies against the get to ask. Finally, the get to response is sent back to the Access Request Processor (Step 5). If the client is affirmed to play out the asked for operation, the Image Processor is summoned with scaling/cropping parameters as information sources (Step 6). The asked for image is recuperated from the Image Store (Step 7) and the Image Processor performs scaling/cropping on the encrypted image. Exactly when the scaling/cropping operations are done, the dealt with image is sent to the Access Request Processor (Step 8). The Access Request Processor plays out the first round of unscrambling on the readied image using the key identifying with the Image User and sends the image to the Access Requester module (Step 9). The Access Requester module on the Image User plays out a moment round of unscrambling and exhibits the readied image to the Image User (Step 10). Observe that the image after the first round of unscrambling on the Cloud Server is still encrypted and the Cloud Server can't take in the mystery data contained in the image. To get to the image in clear-message, a moment round of unscrambling is required using the client side key of the Image User (or Image Outsourcer) for the last decoding round..

IV. ALGORITHM

1. AES

Input: Plain Text

Step1:

Byte state[4,Nb]

State = in

AddRoundKey(state, w[0, Nb-1])

Step2:

for round=1 to Nr-1

SubBytes(state)

ShiftRows(state)

MixColumns(state)

AddRoundKey(state, w[round*Nb, round+1)*Nb-1])

end for

Step3:

SubBytes(state)

ShiftRows(state)

AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1]

Output:Cipher Text

V. RESULT

This system can access the data files of any type and maximum size allowed is 5 MB. In this system user can upload the data that data may be text file,word file,image etc. This data is encrypted and stored on cloud.User can share the uploaded files to another registered user.The analysis is generated based on total number of files shared by the data owners and their access by users.To measure the accuracy of files downloaded by the user we have taken three analysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

parameters.Precision,Recall,Fmeasure.Precision is calculated as total number of (accurate)times file is access divided by total number of files uploaded by the data owners.
precision=no/tcount;
Here no=Number of times file is downloaded correctly by user
tcount=Total number of file uploaded by the data owner
Recall is calculated as total number of files which are not retrieved or incorrectly accessed by the user divided by the total number of files uploaded by the data owner.
Recall=(tcount-no)/tcount
Fmeasure=2*precision* recall /(precision+recall)

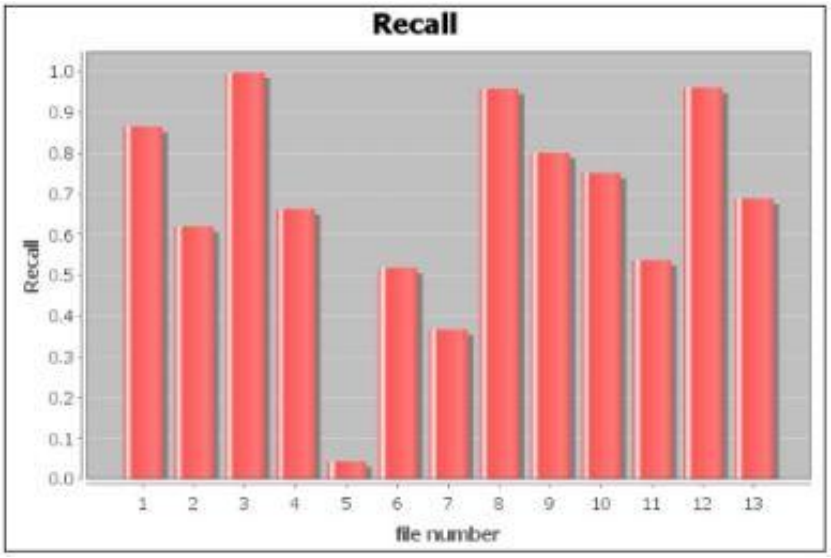

Fig:Recall Graph

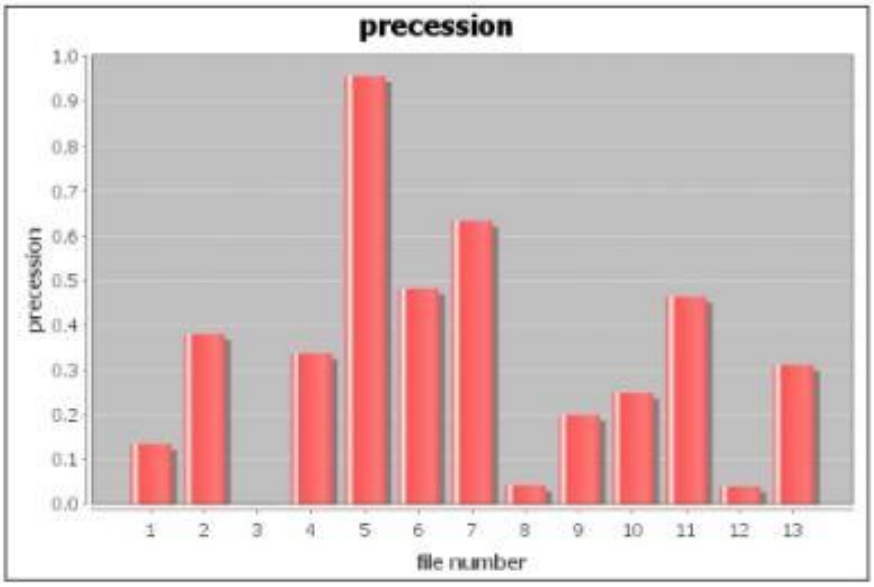

Fig:Precision Graph

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

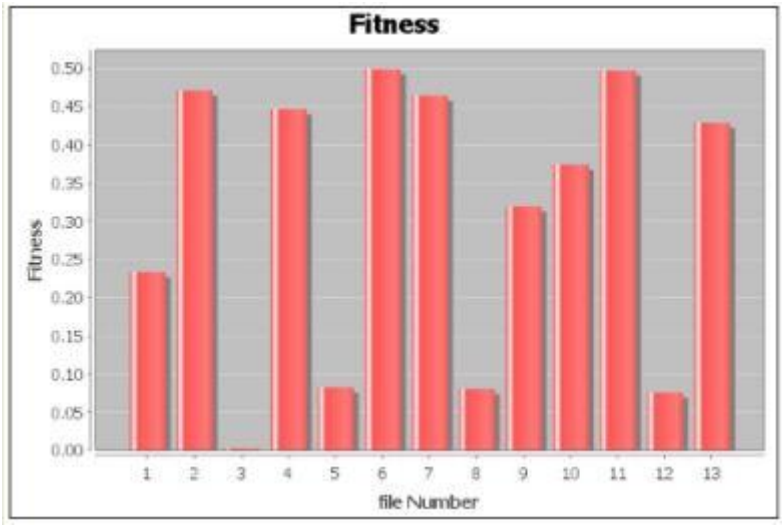

Fig:Fitness Graph

VI. CONCLUSION

Cloud-based image storage has data arrangement issues, which can incite to security disaster. In this framework, we watched out for this issue by proposing 2DCrypt, a changed Paillier cryptosystem-based plan that allows a cloud server to perform scaling and cropping operations without taking in the image content. In 2DCrypt, users don't need to share keys for getting to the image put away in the cloud. In this way, 2DCrypt is suitable for circumstances where it is not appealing for the image client to keep up per-image keys. Also, 2DCrypt is more sober minded than existing plans in perspective of Shamir's mystery sharing since it neither uses more than one datacenter nor acknowledge that various foes could contrive by getting to a particular number of datacenters.First, we proposed a space productive tiling plan that allows the cloud to perform per-tile operations. In 2DCrypt, we put different pixels in a tile, and encode the tile rather than scrambling each pixel uninhibitedly. Furthermore, we updated the adjusted Paillier plan to limit its storage essential. Due to these updates, 2DCrypt requires around 40 times less cloud storage than the gullible per-pixel encryption.

ACKNOWLEDGEMENT

I dedicate all my works to my esteemed guide, Asst.Prof.B. S. Kurhe , whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to Prof.K. S. Kore (H.O.D.ComputerDepartment)who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this paper.

REFERENCES

[1] C. Gentry, A fully homomorphic encryption scheme, Ph.D. dissertation,Stanford University, Stanford, USA, 2009.
[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, Can homomorphic encryption be practical? in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, 2011, pp. 113124.
[3] A. Shamir, How to share a secret, Communications of the ACM,vol. 22, pp. 612613, November 1979.
[4] M. Mohanty, W. T. Ooi, and P. K. Atrey, Scale me, crop me, know me not: supporting scaling and cropping in secret image sharing, in Proceedings of the 2013 IEEE International Conference on Multimedia and Expo,San Jose,USA,2013.
[5] K. Kansal, M. Mohanty, and P. K. Atrey, Scaling and cropping of waveletbased compressed images in hidden domain, in MultiMedia Modeling,ser. Lecture Notes in Computer Science, 2015, vol. 8935, pp. 430441.
[6] C.-C. Thien and J.-C. Lin, Secret image sharing, Computers and Graphics,vol. 26, pp. 765770, October 2002

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[7] T. Bianchi, A. Piva, and M. Barni, Encrypted domain DCT based on homomorphic cryptosystems, EURASIP Journal on Multimedia and Information Security, vol. 2009, pp. 1:11:12, January 2009.
[8] X. Sun, A blind digital watermarking for color medical images based onPCA, in Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, China,August 2010, pp. 421427.
[9] N. K. Pareek, V. Patidar, and K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, vol. 24, pp. 926934, September 2006.
[10] W. Lu, A. L. Varna, and M. Wu, Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization, IEEE Access, vol. 2, pp. 125141,February 2014.
[11] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, Image feature extraction in encrypted domain with privacy-preserving SIFT, IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 45934607, 2012.
[12] J. Yuan, S. Yu, and L. Guo, SEISA: Secure and efficient encrypted image search with access control, in IEEE Conference on Computer Communications, 2015, pp. 20832091.