"A Survey on: A Modified Paillier Cryptosystem-Based Image Scaling and Cropping Scheme"

Mrs. Jadhav Rohini [1], Prof. S. A. Kahate [2]

1 Asst. Prof., Computer Dept., SPCOE, Otur, Pune (India)
2 Prof., Computer Dept., SPCOE, Otur, Pune (India)

ABSTRACT

With the arrival of the cloud computing paradigm and therefore the fast increasing the quantity of on-line services, the web stores not only data for sharing, but also an oversized quantity of private information demanding restricted access and privacy protection. Secure management of private information hold on on-line is an progressively necessary issue, that demands a balance between information confidentiality and handiness. Technologies which will change secure on-line information management square measure attending to be critically necessary for cloud computing to succeed in its full potential. Cloud computing is a rising paradigm giving firms unlimited information storage and computation at enticing prices. It's a cheap model as a result of it doesn't need preparation and maintenance of any dedicated IT infrastructure. Despite its advantages, it introduces new challenges for shielding the confidentiality of the info. Sensitive information like medical records, business or governmental information cannot be holding on unencrypted on the cloud. Firms would like new mechanisms to regulate access to the outsourced information and permit users to question the encrypted information while not revealing sensitive data to the cloud supplier. Progressive schemes don't enable complicated encrypted queries over encrypted information in an exceedingly multi-user setting or information center. To the current finish, would like a second sepulcher, a changed Paillier cryptosystem-based image scaling and cropping theme for multiuser that enable on cloud information center. Due to this multiple user will read and method the image while not sharing any encoding key

Keyword: - *Image Outsourcing, Hidden Image Processing, Encrypted Scaling and Cropping, Paillier Cryptosystem*

1. INTRODUCTION

The expansion of cloud storage and computing platforms permits users to source storage and computations on their information, and permits businesses to dump the task of maintaining data-centers. However, issues over loss of privacy and business value of personal information are an amazing barrier to the adoption of cloud services by customers and businesses alike. Superb thanks to assuage these privacy issues is to store all information within the cloud encrypted, and perform computations on encrypted information. to the present finish, want an cryptography scheme that enables meaningful computation on encrypted information, particularly a homomorphic cryptography scheme.

1. 1 HOMOMORPHIC ENCRYPTION SCHEME

Here describe variety of concrete applications and functions to be enforced to produce cloud services within the medical, financial, and advertising sectors. For a cloud service managing electronic medical records (EMR), consider a art movement situation wherever devices continuously collect important health data, and stream them to a server who then calculate some statistics (over these measurements, and over the course of time) and presumptively decides on the course of treatment (e.g., whether or not the dose of medication should be changed). The degree of the information concerned is large, and thus, the patient presumptively doesn't need to store and manage all this information locally; she could favor to use cloud storage and computation. to guard patient privacy, all the information is uploaded in encrypted kind, and so the cloud should perform operations on the encrypted information so as to come back (encrypted) alerts, predictions, or summaries of the results to the patient. Ideally, one would like to use the absolutely homomorphic cryptography theme to perform any sort of computations over encrypted However; current homomorphic cryptography schemes don't seem to be computationally practical. Once working on encrypted information, usually plenty of attention is paid to the particular theme while not considering key management, a side important for organizations. In a typical organization, provision a similar key to all or any workers, who need to share information, isn't possible. In a perfect situation, every employee should have her own personal key that can be used to access information encrypted by the key of the other use. This situation is commonly cited because the full-fledged multiuser model. When the worker leaves the organization, the employee's key should be revoked and the employee should not be ready to access any information (including her own data) any longer. However, the information should be accessible to employees still holding valid keys.

To protect image confidentiality and integrity, one will use secret image sharing [3] to cover a picture (i.e., the key image) from anyone of the datacenter by distributing the shares (i.e., the shadow images) across multiple datacenters. Existing proposals for secret image sharing, particularly, those based on Shamir's secret sharing scheme and multi-secret image sharing schemes, mainly focus on the trade-off between potency and security, and don't easily support image operations on the shadow pictures. Two vital image operations on large pictures are scaling and cropping. Downloading an oversized image, like a histopathological image (whose size may be within the order of tens of GBs) to users might not be continuously possible. Users might want to preview a scaled down version of the image before deciding whether or not to transfer the image. Further, users could need read a specific region of interest within the image, within which case; a cropped region ought to be downloaded. These 2operations, scaling and cropping, may be combined to support zooming and panning, two natural user interactions to explore massive pictures. Supporting scaling and cropping with secret image sharing is non-trivial. A naive solution would be for the info source to create multiple secret pictures at totally different resolutions (to support scaling) and to divide every secret image into severally decodable tiles (to support cropping). These tiles are then secret-shared across the datacenters..

2. SYSTEM MODEL:

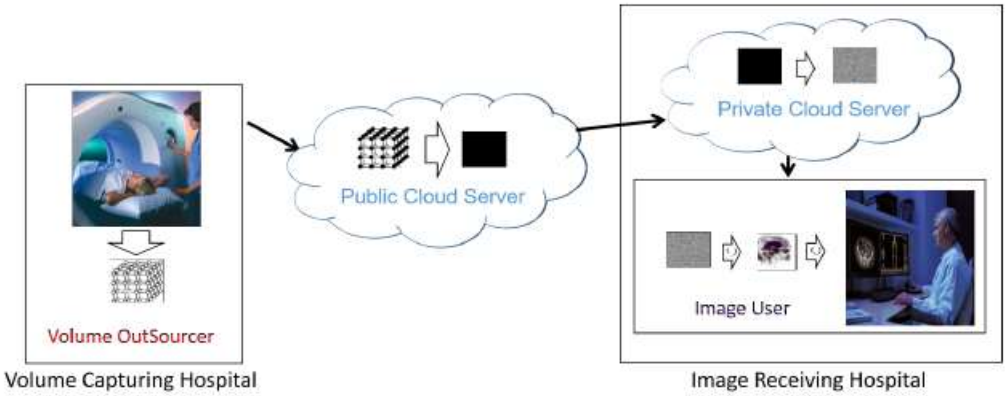

Figure 1: Cloud-based rendering of medical data.

Volume Outsourcer: This entity outsources the storage and rendering of volumes to a third-party cloud provider. It might be a personal or a part of a company. within the latter case, users can act as Volume Outsourcers. Typically, this entity owns the volume. the volume Outsourcer can store new volumes on a cloud server, delete/modify existing ones and manage access control policies (such as read/write access rights).In our state of affairs, the quantity Outsourcer is an element of a volume capturing hospital

- **Public Cloud Server:** A Public Cloud Server is an element of the infrastructure provided by a cloud service supplier, like Amazon S31, for storing and rendering of volumes. It stores (encrypted) volumes and access policies accustomed regulate access to the degree and the rendered image. It performs most of the rendering on keep volumes and produces the partially rendered information.

- **Private Cloud Server:** The private Cloud Server sits between the public Cloud Server and the rendering requester. It will be a part of the infrastructure, either provided by a personal cloud service supplier or maintained by a company as a proxy server. The non-public Cloud Server receives partially rendered information from the public Cloud Server and performs remaining rendering tasks on the degree. It then sends the rendered image to the rendering requester. Note that the non-public Cloud Server doesn't store information; it solely performs minimal rendering operations on partially rendered information received from the public Cloud Server.

- **Image User:** This entity is permitted by the volume Outsourcer to render a volume keep in the Public Cloud Server. during a multi-user setting, a picture User will (i) render a picture (in encrypted domain) that may be accessible by different Image Users, or (ii) access pictures rendered by different Image Users. In each cases, Image Users don't got to share any keying material.

- **Key Management Authority (KMA):** The KMA generates and revokes keys to entities concerned within the system. for every user (be a Volume Outsourcer or Image User), it generates a key combine containing the user-side key and therefore the server-side key. The server-side secret's firmly transmitted to the public Cloud Server, whereas, the user side secret is either sent to the user or private Cloud Server depending on whether or not the user could be a Volume Outsourcer or Image User. Whenever needed (say in key lost or taken cases), the KMA revokes the keys from the system with the support of the public Cloud Server

3. SYSTEM ARCHITECTURE:

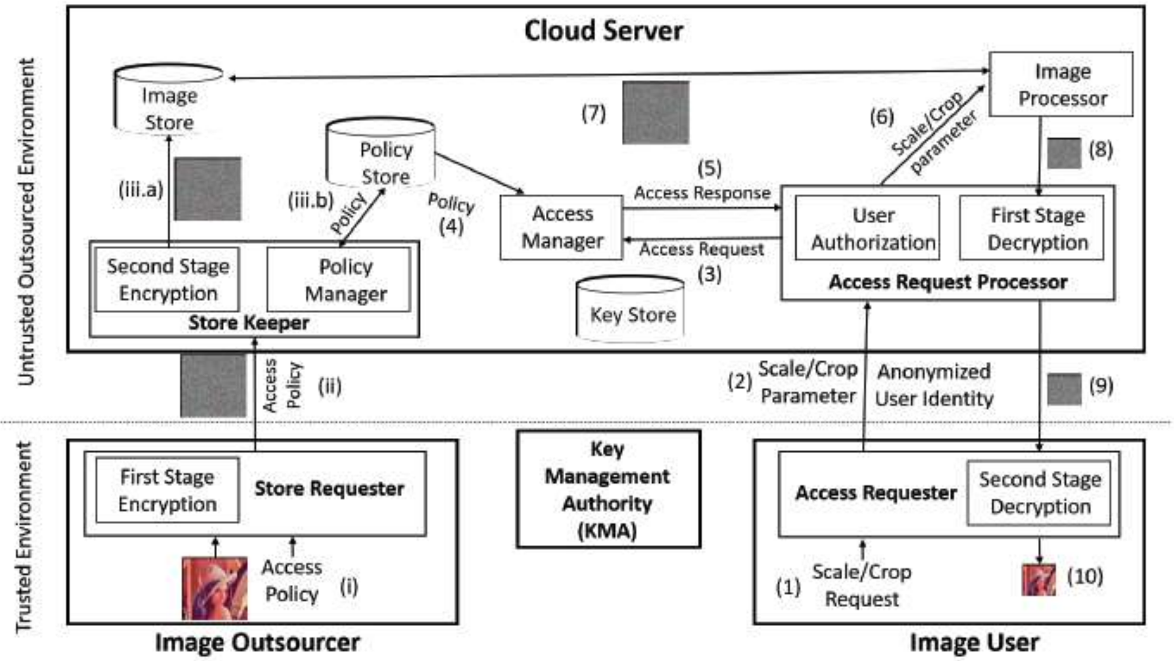

Figure 2: The architecture of 2DCrypt: a cloud-based secure image scaling and cropping system.

3.1 EXISTING SYSTEMS

- ❖ An Image Outsourcer is responsible for addressing security and privacy concerns attached to image outsourcing. To achieve this, the Image Outsourcer encrypts the image before sending it to the cloud datacenter. Further, the Image Outsourcer can store new images on a cloud server, delete/modify existing ones, and manage access control policies (such as read/write access rights) to regulate access to the images stored on the cloud server.

- ❖ In order to provide the multi-user support, we extend the modified Paillier cryptosystem such that each user has her own key to encrypt or decrypt the images. Thus, adding a new user or removing an existing one will not require re-encryption of existing images stored in the cloud.

- ❖ 2DCrypt is more practical than existing schemes based on Shamir's secret sharing because it neither employs more than one datacenter nor assumes that multiple adversaries could collude by accessing a certain number of datacenters.

3.2 PROPOSED SYSTEMS

- ❖ The use of cryptosystems for hiding images is a well-studied area. A number of approaches, including but are not limited to, Public Key Cryptosystem (PKC), watermarking, Shamir's secret sharing and chaos-based encryption, have been proposed to protect images.

- ❖ To allow cloud datacenters to perform operations on the encrypted image, partial homomorphic cryptosystem-based solutions have been proposed. A partial homomorphic cryptosystem exclusively offers either addition or multiplication operations. Paillier, Goldwasser-Micali, Benaloh, Shamir's secret sharing are among partially homomorphic cryptosystems that support addition. Few works have been proposed for searching encrypted images based on dynamic extraction of image features.

- ❖ Although proposed tile-level encryption scheme 2DCrypt can have less computational and storage overheads than the naive per-pixel encryption, the flexibility of selecting an individual pixel is lost.

➢ System Configuration

- **H/W System Configuration:**

Processor	-	**Pentium –III**
❖ Speed	-	1.1 Ghz
❖ RAM	-	256 MB (min)
❖ Hard Disk	-	20 GB
❖ Key Board	-	Standard Windows Keyboard
❖ Mouse	-	Two or Three Button Mouse
❖ Monitor	-	SVGA

- **S/W System Configuration:**

❖ Operating System	:	Windows95/98/2000/XP
❖ Application Server	:	Tomcat5.0/6.X
❖ Front End	:	HTML, Java, Jsp
❖ Database	:	Mysql
❖ Database Connectivity	:	JDBC

4. ADVANTAGES

- To take full advantage of the input space allowed by the proposed cryptosystem, introduce a concept of tiling to group a set of pixels.
- A tile can be encrypted instead of encrypting each pixel. Using the tiling in 2DCrypt, save the space and decrease the number of required encryptions and decryptions by a factor of the tile size.
- Here proposed a space efficient tiling scheme that allows the cloud to perform per-tile operations. In 2DCrypt, put a number of pixels in a tile, and encrypt the tile instead of encrypting each pixel independently

5. CONCLUSIONS AND FUTURE WORK

Cloud-based image processing has data confidentiality issues, which can lead to privacy loss. In this paper, addressed this issue by proposing 2DCrypt, a modified Paillier cryptosystem-based scheme that allows a cloud server to perform scaling and cropping operations without learning the image content. In 2DCrypt, users do not need to share keys for accessing the image stored in the cloud. Therefore, 2DCrypt is suitable for scenarios where it is not desirable for the image user to maintain per-image keys. Furthermore, 2DCrypt is more practical than existing schemes based on Shamir's secret sharing because it neither employs more than one datacenter nor assumes that multiple adversaries could collude by accessing a certain number of datacenters.

6. ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere gratitude to my Project Guide Prof.S.A.Kahate for his encouragement, guidance, and insight throughout the research and in the preparation of this paper He truly exemplifies the merit of technical excellence and academic wisdom. His extensive knowledge, serious research attitude and encouragement were extremely valuable to me. I also appreciate not only for his full time, timely and valuable advices, but also for his continuous scheduled follow up and valuable comments during my research work.
I should also like to acknowledge the contribution of my Principal Dr.G.U.Kharat and Head of Department Prof. Deokate G. S.

7. 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. 113–124.

[3] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612–613, 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 & Expo, San Jose, USA, 2013.

[5] K. Kansal, M. Mohanty, and P. K. Atrey, "Scaling and cropping of wavelet-based compressed images in hidden domain," in MultiMedia Modeling, ser. Lecture Notes in Computer Science, 2015, vol. 8935, pp.
430–441.

[6] C.-C. Thien and J.-C. Lin, "Secret image sharing," Computers and Graphics, vol. 26, pp. 765–770, October 2002.