ISSN No:-2456-2165

2DCrypt: Image Scaling and Cropping Without Physical Interface

Sudhakara Reddy M[1]
Computer Science and Engineering
Nagarjuna College of Engineering and Technology

Sindhuja M[2]
Computer Science and Engineering
Nagarjuna College of Engineering and Technology

Sireesha K[3]
Computer Science and Engineering
Nagarjuna College of Engineering and Technology

Tejaswini M[4]
Computer Science and Engineering
Nagarjuna College of Engineering and Technology

Geethika R V[5]
Computer Science and Engineering
Nagarjuna College of Engineering and Technology

Abstract:- In this project we are using the concept of encryption and decryption. Firstly, we use encryption to store the data in the cloud without any physical interface later we use decryption to decrypt the data from the cloud. If you want the decrypt the data from the cloud. We use key to decrypt. Any user can easily fetch the decrypted message with the key provided by the authorized user but not by the unauthorized users.

For Example, Basically we store the data manually as we need to maintain the records physically so by this we may face many issues like data theft or data may be replaced. So, overcome all this scenario we can store the information in the cloud for maintaining data and to secure the data.

I. INTRODUCTION

Cloud computing is a platform for accessing the unlimited and the computational resources with this client access fast and reliable hardware. Now a days, building applications for multimedia content infrastructure are common in cloud providers.

Images may contain personal information if image is not protected in cloud then it shows an unauthorized access or you cannot access this image.

If once the image is stored in cloud we cannot encrypted the images and we cannot perform any operations of cropping, zooming and penning etc.

If the any user is downloading the encrypted images some encryption techniques should be downloaded before so that the user can easily perform the operations for the encrypted images. If the downloaded resources are not then the user cannot perform any operations.

Big Data is a formal product that has a advanced research efforts to reallocate the ITC business and cloud computing in the olden years. The technologies that developed in ICT technologies are communication, storage, computation. It has a innumerous information that helps in business, science. These roles helps to generate, think about the information and discover the worth of the data. Now a days, ITC industries and scientists are using the petabytes of package of information that stored in cloud computing. For examples, in companies, Google, yahoo!, Amazon uses a large amount of data in our daily life for supporting information in useful manners.

In olden days, many technologies are introduced to change a large amount of information, i.e. ranging from terabytes to petabytes of information. These techniques allows users to do data in parallel ways.

Now, there are several isuses that are facing in developing Map Reduce i.e. load balancing, exchanging information among large sets of data allocated around one-third of time particularly in job running time in the Hadoop especially on Facebook. Here, our main aim is to focus on big data that is one of the needed communication in distributed systems.

II. 2D ENCRYPTION

The 2DEncryption Mode(2DEM) is elobrated to 1DEncryption. The 2DEncryption mode takes and analyzes its input as a images, photos and also data in the binary format. The 2DEM modes is mainly used on 2D data. Information is useful and supplied to two-dimensional array of bytes called “Data”. It can be in the form of bytes. These bytes are access in the form of rows numbers and column numbers.

The Data Encryption Standard (DES) is a symmetric-key block cipher. It is announced by National Institute of Standards and Technology (NIST). It has a block of 64 bits and its key-length is 64 bits. DES has effective and useful key length of 56 bits.

ISSN No:-2456-2165

➢ *Decryption*

Decryption is the method of using encrypted text or encoded data or other information. It can converting the encoded data into the text format or the computer can easily analyze and read it. These data can be modified by using the particular keys or codes. Decrypted is normally reverse process of encryption. An authorized user can also decrypt information because decryption requires a password or secret keys to retrieve or store the information.

➢ *Encryption Process*

Normal File -> Encrypt using RNS ->F1 (encrypted by RNS)
F1 (encrypted by RNS) -> Encrypt using DES -> F2 (Encrypted by DES & RNS)

➢ *Decryption Process*

F2 -> Decrypt using DES ->F1 (encrypted by RNS)
F1 (encrypted by RNS) -> Decrypt with RNS -> Normal File.

The images are used and transformed in scaling and cropping operations. It will be used in encrypted images. These contains two drawbacks:

- For each image, n shares are created and sent to the cloud, which improves the capacity of storage usefulness and the processing capacity.
- There is no security against collapsing: if k data centres collapse then the original image can be stored and secured.

In my project, we are going to implement a new encrypted technique. That we call it as a 2DEncrypted. 2DEncryption is the new technique of 1DEncryption. It has many advantages as well such as good security and we can analysis it practically also. It can also perform some mathematical operation in a vivid and easy manner that every one able to understand and analyze it. It plays a key role for storage purposes, cloud environment, storing and hiding the images.

Key management is important and also plays a major role in many IT sectors and institutes. Employees want to distribute the information among their collegues. In this process, it is difficult to send same key among them. And also sending same key to all employees also leads to many disasters if the authorized employee may leave the IT company. Again another new key should be generated and information must be again transformed by using new key. In this situation, every employee should contains their personal key to login and access the information encrypted by another employee's key. So, this process is called Full-Fledged-Multi-User models.

- Encryption is used for encoding a message or information that only authorized users can login and access the information.
- In encrypted algorithm, Algorithm produces a readable text (cipher text) that can only read if it is decrypted.
- An encrypted scheme usually uses a pseudo-random encryption key produced by algorithm.
- The 2D-Encrypted Mode (2DEM), it is the elobration of 1D encryption to the 2D encryption.

➢ *Many Service in Cloud Computing*

Cloud computing is generally used in 2 ways. Either on cloud locations or on the service of the cloud is offering. Based on cloud computing we use as

- Public
- Private
- Hybrid
- Community cloud

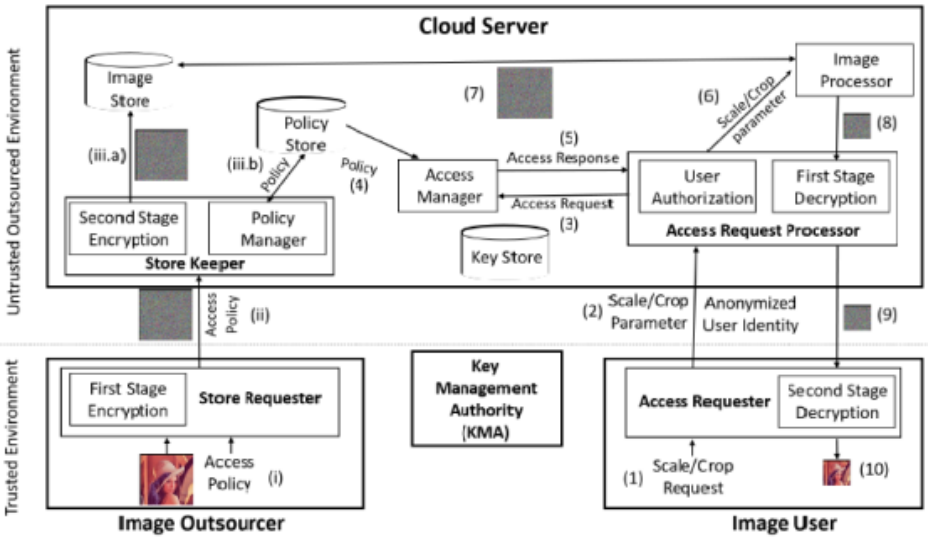
The services of cloud is various types as

- Iaas (Infrastructure-as-a-service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- Security, Storage, Database

ISSN No:-2456-2165

III. TREEDIAGRAM

➢ *Block Diagram*



The Architecture of 2DCrypt: a Cloud-Based Secure Image Scaling and Cropping System

Fig 1

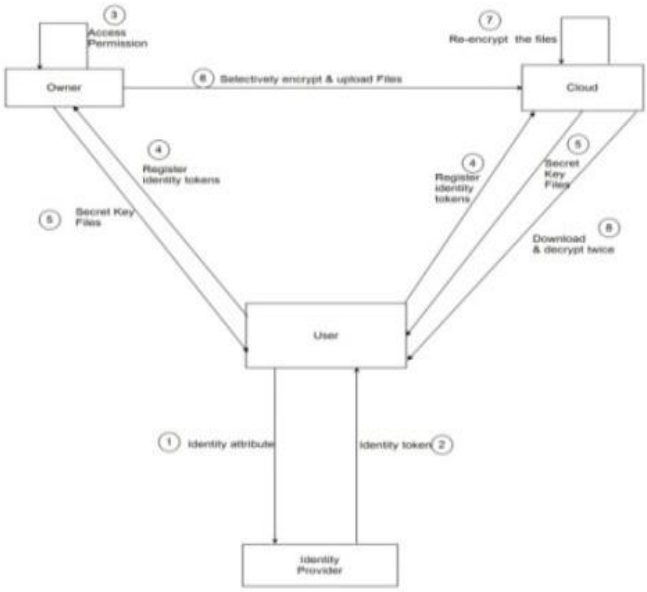


Fig 2

➢ *Software Requirements*

Logitech
Pentium IV 2.4 GHz

➢ *Hardware Requirements*

Windows
Java (JDK 1.7)
Net Beans
JMF

➢ *Our Model and State of Art*

In our model, we focus on panning, scaling and cropping through which we can navigate the large images and the images which have been encrypted in the cloud and these cannot be leaked. In the cloud the information can be leaked easily if it is not encrypted. But in cloud you can replace the data. Cloud is not deployed to infrastructure. But for authorized users they can change the data which is there are of before.

In this over the encryption data we perform the operations by using the Shamir secret sharing for scaling and cropping operations. For extending the work of them sharing the secret images and data distributed among the multi cloud providers to recover the original images out the many shared images and to be retrived

IV. CONCLUSION

2DCrypt is used in many ways. The main scenario, is used to elobrate the work for compressed images. The main advantages is 2DCrypt is approximately 40 times less of cloud storage than the per-pixel encryption. In our project, we are using the future work for video processing in encrypted domains. 2DCypt uses in a cloud server for scaling and cropping techniques. Theses project is very interesting, if we use these properties in many images for further decrease of it.

In my project, is mainly based on IAS (Infrastructure as a service). It is a lowest level. The Iaas provider are as Amazon, Google Compute Engines. Infrastructure as a service (Iaas) mainly useful in business sectors via web architecture, servers and connections. Iaas cloud uses a complexity to solve the complex information. Encryption can be used to secure and store the information on computers and storage devices. Encryption has been used in militaries and government to provide communication among them.

REFERENCES

[1]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, 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 IEEEInternational 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.
[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. 1:1–1:12, January 2009.
[8]. X. Sun, "A blind digital watermarking for color medical images based on PCA," in Proceedings of the IEEE
[9]. International Conference on Wireless Communications, Networking and Information Security, Beijing, China, August 2010, pp. 421–427.
[10]. N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, pp. 926– 934, September 2006.
[11]. 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. 125–141, February 2014.
[12]. 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. 4593–4607, 2012.
[13]. 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. 2083–2091.
[14]. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology EUROCRYPT, 1999, vol. 1592, pp. 223–238.
[15]. S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.