Reducing Storage Cost using Secure Image Deduplication

Ketakee Dangre[1], Mr. Amit Pampatwar[2], Ms. Raana Syeda[3]
[1]Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Abstract : *Data deduplication is an important aspect for Cloud Storage Providers (CSPs) since it allows them to remove the identical data from their storage successfully. Convergent encryption is used to securely eliminate duplicate copies on the encrypted data. The Message Locked Encryption (MLE) scheme is frequently mentioned in research papers for achieving data de-duplication securely. Researchers have introduced Message locked Encryption based protocols which provide secured deduplication of data, where the data is in text form. Multimedia data such as images, which are larger in size compared to text files, have not been given much attention. Applying secured data deduplication to such data files could significantly reduce the cost and space required for their storage. This helps in reducing maintenance cost as well for the storage providers and hence improved performance and cost effective.*

Keywords*: Cloud Storage, Data Security, Image Deduplication.*

I. Introduction

In this paper we use a secure way of deduplication scheme for near identical (NI) images with the Dual Integrity Convergent Encryption (DICE) protocol, which is a variant of the MLE (Message Locked Encryption) based scheme. In the proposed scheme the blocks that are common between two or more NI (nearly identical) images are stored only once in the storage. As compared to other techniques DICE protocol saves large amount of memory on cloud storage as many techniques perform deduplication on entire image but in DICE protocol an image is disintegrated into blocks and the DICE protocol is applied on each and every block separately rather than on the entire image. In this we use secure block level image deduplication method that eliminates the near identical images in encrypted form, thus protecting the confidentiality of the images.

Our core idea is to divide the image into blocks and employ the DICE protocol on each block separately. Each block is encrypted using AES with a key that is obtained by hashing the image blocks. There are several other techniques for Data Deduplication SPSD (Secure Perceptual Similarity Deduplication), CSPD (Client Based Secure Provable Deduplication), Image Compression.

II. Figures And Tables

Data given bellow describes information about work done and screenshots of the same for explaination and understanding of project. It is developed in Python and MySQL used to store data of image.

1. Home Page

This window contains login account for two users

1.1 Users

In this only an authorised person can access data. Person can perform image related operation like upload and download if he is an authentic user.

1.2 Cloud service Provider

Cloud service Provider gives access to the server side authority. CSP is responsible for managing storage of data. We will store our data on cloud which can be access from any remote location.

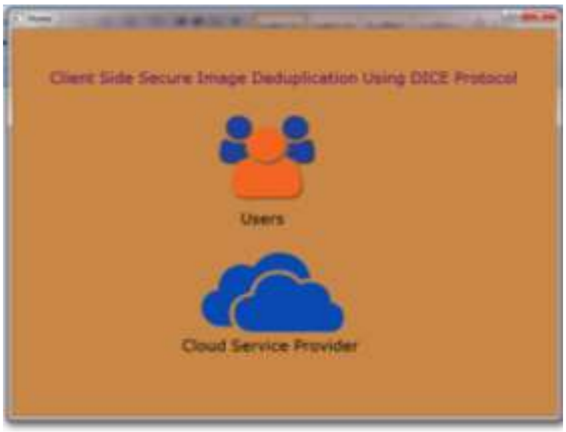

Fig 1. Home Page

2. Login Window

By using this window already registered user will be able to access next window of the project.
After entering valid user name and password user will get further access to the system.

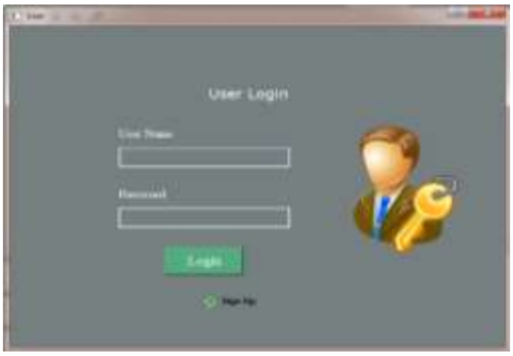

Fig 2. Login Window

3. Registration Window

In Registration window new user can enter their information for creating a new account. It contains various fields like name, username ,password , Email and mobile number.
Valid username and password are required to get access to the system and its stored information.

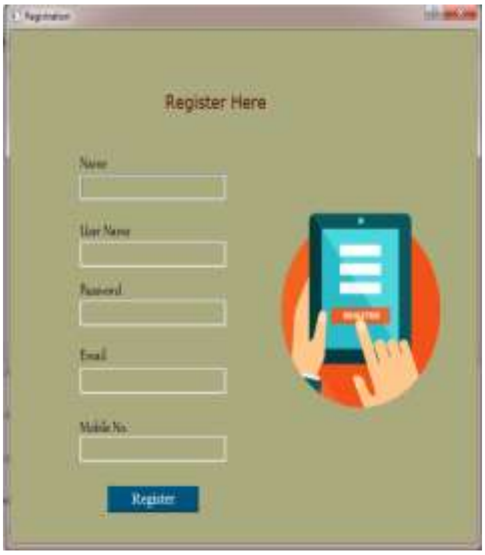

Fig 3. Registration Window

4. UserHome

This window contains two buttons which peform operation of Image Upload and Image Download. Its a two way communication process between user and server where user will save or upload data on cloud and in Image Download option user can download image from server. Description of Image Upload given in next window.

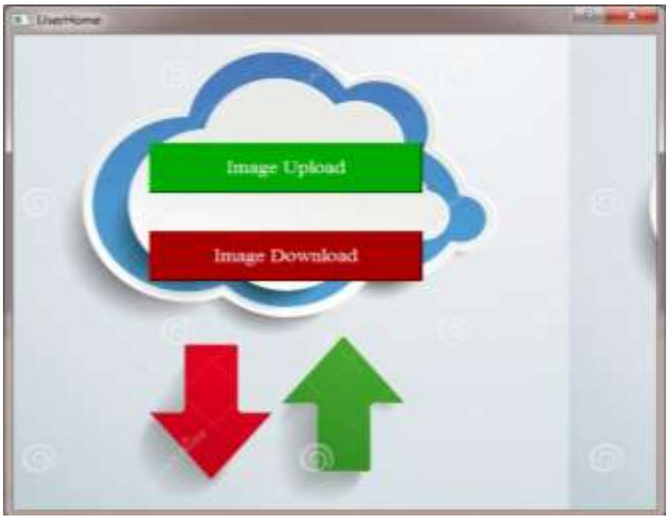

Fig 4. UserHome Window

5. File Upload Window

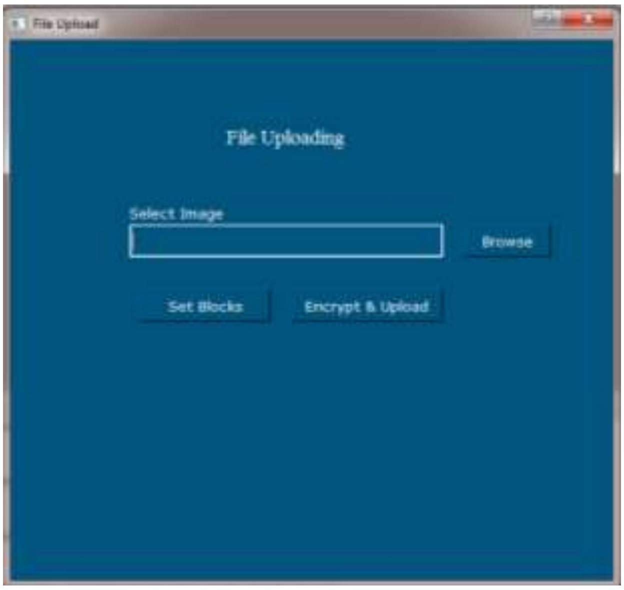

Fig 5. File Upload window

Upload operation used to store image on cloud or local database here we use MySQL for storing data. Set Blocks button will perform operation on image by dividing image into blocks. Here we use 6*6 blocks. This blocks are further used to encrypt and upload on cloud.

Currently working on Cloud Service Provider module, it will give information about Storage Files and Graph. It provides information about data stored on cloud and graph will show the difference between Storage spaces required for data without performing deduplication and after applying Deduplication scheme.

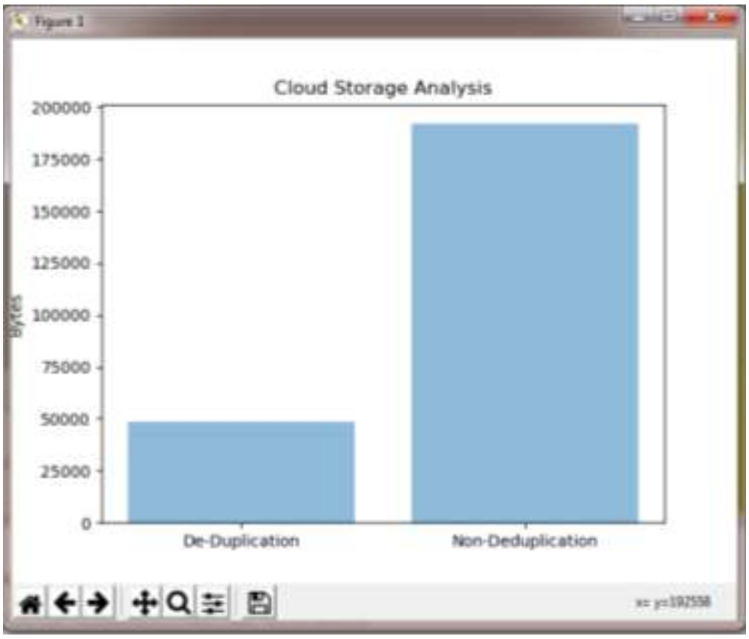

Fig 6: Storage Graph

III. Conclusion

DICE protocol is one of the best ways to achieve image de-duplication and securely store image on local storage or cloud platform. DICE protocol is secured over MLE, SPSD and CSPD techniques as it uses image deduplication at the block level. It performs deduplication on different types of images. We found that the greater the similarity of the images, the smaller the number of blocks stored at the cloud. However, the constraint here was that the images were nearly identical with small variations among them. . In future we would like to add more image operations like scaling, rotation, cropping, multiple viewpoints, lighting conditions and compression with different file formats, and tests them at the cloud.

Acknowledgements

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

References

[1]. Ashish Agarwala, Priyanka Singh, Pradeep K. Atrey,   "Client Side Secure Image Deduplication Using DICE Protocol" in 2018 IEEE Conference on Multimedia Information Processing and Retrieval, New York

[2]. A. Agarwala, P. Singh, and P. K. Atrey, "DICE: A dual integrity convergent encryption protocol for client side secure data deduplication," in *IEEE International Conference on Systems, Man, and Cybernetics*, Banff, Canada, 2017, pp.2176–2181.

[3]. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Messagelocked encryption and secure deduplication," in *Advances in Cryptology – 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Athens, Greece, 2013, pp. 296–312.

[4]. F. Rashid, A. Miri, and I. Woungang, "Secure image deduplication through image compression," *J. Inf. Secur. Appl.*vol. 27, no. C, pp. 54–64, 2016.

[5]. D. Li, C. Yang, C. Li, Q. Jiang, X. Chen, J. Ma, and J. Ren, "A client-based secure deduplication of multimedia data," in *IEEE International Conference on communications*, Paris, France, 2017, pp. 1–6

[6]. X. Li, J. Li, and F. Huang, "A secure cloud storage system supporting privacy-preserving fuzzy deduplication," *Soft Computing*, vol. 20, no. 4, pp. 1437–1448, 2016.

[7]. Mihir Bellare, Sriram Keelveedhi, Thomas Ristenpart,   " Message-Locked Encryption and Secure Deduplication" Eurocrypt 2013.

[8]. M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in *Public-Key Cryptography – 18th IACR International Conference on Practice and Theory in Public-Key Cryptography*, Gaithersburg, MD, USA, 2015, pp. 516–538.

[9]. E. Torres, G. Callou, G. Alves, J. Accioly, and H. Gustavo, "Storage services in private clouds: Analysis, performance and availability modeling," in *IEEE International Conference on Systems, Man, and Cybernetics*, Budapest, Hungary, 2016, pp. 3288–3293.