IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

Image and Text Encrypted Data with AuthorizedDeduplication in Cloud

Prof. M.B. Yelpale[1], Akhil V[2], Devyani Sharma[3], Shashank Nathe[4], Aniket Lodhe[5]
Faculty, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, India[1]
Students, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, India[2,3,4,5]

Abstract: *In this study, role re-encryption is employed in a secure role re-encryption system to minimize data leakage and deduplication. It also looks for evidence of ownership to see whether the user is an authorized one. This is for the sake of effectiveness. The role re-encryption approach involves sharing the access key for the associated authorized user in order to access a specific file without exposing personal information. We use both the avoid use of text and digital visuals in our endeavor. Personal photographs, for example, are stored on our mobile phones, portable devices, computers, and other gadgets. As these photographs must be kept confidential, we are encrypting them. Nowadays, the text file is equally significant for users. It must be kept safe on a cloud server. Digital photographs must be safeguarded during transmission, but personal identity information such as copies of a pan card, passport, ATM card, and so on, should be stored on a single wnpc. To minimize duplication in our proposed system, we are securing the text file and picture data.*

Keywords: Deduplication, Encryption, Decryption, AES, MD5, etc.

I. INTRODUCTION

As social media grows in popularity and use, people are posting, sharing, and sending data in record numbers. The majority of software apps, social media sites, and businesses utilise cloud services to store their massive amounts of data. Files with the same content might be uploaded by the same or different users, causing the system to store the samefiles again and over, wasting the relatively costly storage space purchased from cloud service providers. Existing cloud storage companies' de-duplicate data to minimize wasting space, which benefits both themselves and their consumers. De-duplication may save backup storage requirements by up to 9095 percent [11] and regular file system storage requirements by up to 68 percent. Encrypting the same files with different keys entered by users results in the generation of different cypher messages, even though the underlying plain text is the same. 1 As a result, classical encryption fails in data de-duplication on encrypted files. However, encryption is expected to protect the security and secrecy of data.

Previous de-duplication technologies, however, cannot guarantee the data's robustness. Furthermore, many de1duplication technologies require the data owner to all be brought online 1 in order to exchange a convergence key, therefore decryption cannot be performed just at time it is requested. Previous systems did not address storage server assaults and data retrieval in such attacks. In this research, 1 we propose a de-duplication method which is based on an erasure correction technique that splits the file into shards and distributes it over several cloud storage providers' servers. Even if only one of the servers is attacked by an intruder, the system can re-generate the original files using the remaining of repaired shards. Like a outcome, the system can guarantee the encrypted file's dependability and robustness.

II. MOTIVATION

Encrypted file deduplication schemes can enhance cloud storage. space utilization while still protecting file privacy.We Try to access File Securely to Decrypted format.

III. LITERATURE SURVEY

Chippy Jacob, Rekha V. R "SECURED AND RELIABLE FILE SHARING SYSTEM WITH

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

DEDUPLICATIONUSING ERASURE CORRECTION CODE".

[1] Effective file system storage and administration is critical these days to avoid wasting the storage capacity suppliedby cloud providers. Data deduplication is a frequently used technique that allows only an unique copy of the file to be saved and thus prevents file duplication in cloud services. It contributes to the reduction of storage network storage used by cloud services, resulting in significant cost savings for cloud service subscribers. Today, we have kept data in secure manner to maintain security. Thus, cryptographic algorithms by data owners using their own keys makes de- duplication impossible for cloud service subscribers because cryptographic protocols with either a key converts data into an undecipherable format called cypher text, and thus encrypting the same data between different codes may result in different cypher texts.

However, de-duplication and encryption must function in tandem to enable secure, permitted, and optimal storage. Based on the user's access set and asset privilege set, we present a technique for data de duplication on encrypted data such as text, photos, and even video files saved in the cloud in this work. This study presented a de-duplication technique for distributing files across many servers. The system re-constructs the files usinga Reversal Correcting Code approach, even if sections of both the records are lost due to an assault on any server. As anoutcome, the suggested system can improve the confidentiality and dependability of encrypted files.

fshan Mulla∗, Amol Baviskar†, Jaypal Baviskar‡ Mugdha Gulati and Amruta Mhatre, "Wavelet Based Image-Text Fusion Algorithm for Encrypted Message Transmission".

[2] The demand for resilient algorithms has increased due to higher demand for secure communication over the network. The algorithms must be highly effective in order to secure the confidentiality, authenticity, and integrity of thecommunications sent. In this research, we implemented a mechanism for sharing secret messages by encrypting them incoloured photographs processed using the Dwt (DWT). The approach employs a novel sub band elimination strategy to exploit the fundamental features of DWT and insert a text message in the deleted sub-band. The method of band minimization is guided by determining the energy output of each band. The suggested technique assures that the text message is only received by an authenticated recipient who has the access key. This technique has been shown to include a reliable transmission of information along with suitable compression ratios. This publication also provides a full examination of the algorithm.

Jitha Raj.T, PG Scholar, "A Survey Paper on Various Reversible Data Hiding Techniques in Encrypted Images"

[3] A process of concealing data is known as data hiding. Material could be concealed but use a number of methods. Voice, video, images, writing, and picture can all be used to hide data. The method is also called as cryptographic, which is really 1 the process of placing data within other data. Typically, visuals, particularly digital graphics, are used to protect secret. There are various approaches available for encoding information in photographs. Some approaches will embed data, but the visual will just be distorted 1 as a result of the embedding; some techniques may embed only a tiny quantity of data; and some procedures will induce distortion during data extraction. As a response, this document describes the various ways for embedding and extracting data.

Arun K Mohan, Saranya M R, "Multi-level Encrypted Reversible Data Hiding using Histogram Shifting for Configurable Embedding Rate".

[4] This paper proposes a reverses dataset hiding (RDH) method for grey cover images with very sensitive cover material. By combining the histogram shifting approach to incorporate secret bits in confused covers, the strategy uses the least amount of computing cost, having cover confusion handled by the linear map function. A multi-level system embedding procedure is utilised to obtain high capacity or flexible embedding rates while incorporating the secret bits. Confused covers with concealed data alone or tagged stego covers prepared with any transpose algorithm for confusion are used in a range of statistical, plain text, and brute force assaults. As a result, we proposed embedding information ina puzzled cover, followed by a successive multi-level encryption scheme using the Schwarzenegger cat mapper and unstable systems. The proposed system in a cryptosystem gained extremely strong immunity against all forms of attacks, but it jeopardized a separable method of action.

D. Saravanan, "Effective communication through Image Code Technique".

[5] While information is communicated through images, camouflaging of double images is required. Technology facilitates communication; most communication today takes place via an open network, and as a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

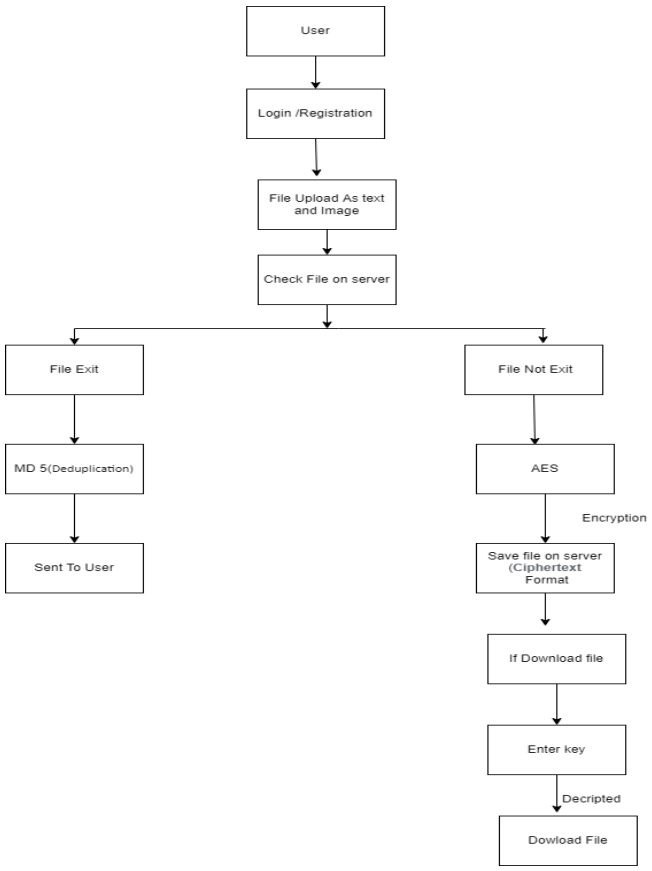
function, risks are increasing on a regular basis. This study introduces a new technique known as the flow code procedure technique. Given a binary image, it is converted to text and encrypted using the flow code procedure. The existing picture transformation is done through image compression, and this compress image alone never delivers security. Images mustbe translated into code before they may communicate in the network. Images are transformed to text using a character system table in this case. The fundamental advantage of the suggested technique is that even the user does not need to remember any keys. The scientific values show that the suggested technique outperforms existing techniques.

IV. PROPOSED SYSTEM

To The working of the proposed is based on the fact that the texts present in images have some unique features weuse Following Module in Proposed System.

- **Deduplication**
  For the Deduplication we use MD5 Algorithm. If deduplication Occur in file, then we sent to user again and if filecontain is not deduplication, then store file.
- **Encryption:**
  File contain is unique That time AES algorithm working and store file in encrypted format.
- **Decryption:**
- If user want or access file or download file in original format that time AES algorithm download file in decryptedformat.

V. SYSTEM ARCHITECTURE



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

VI. ALGORITHM

AES:

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithmis considered secure, it is in the worldwide standard.

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

MD5:

The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been foundto suffer from extensive vulnerabilities.

VII. AIM AND OBJECTIVES

The model for encryption and decryption of an image is designed with some objectives:

- For transmission of the image and text file based on data as well as storage it should have confidentiality andsecurity by using suitable key.
- To study the architecture of the image file.
- To encrypt the image file by developing the application.
- Eventually, the image is focused on most famous file type of image format i.e., JPG and PNG.
- The image is focused to JPG and PNG file type which is the most famous type of image format.
- The application must be simple, easy to use and powerful.
- Many factors have to be considered in order to develop the application such as processing speed of image, thestrength of encryption result and ease of use to end users.

VIII. METHODOLOGY

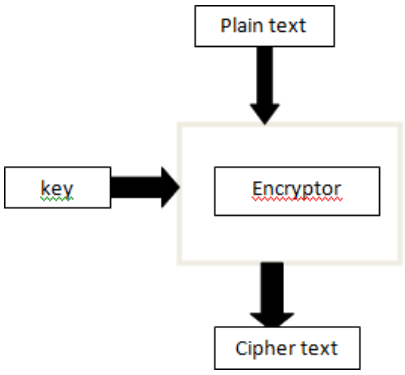


Figure 1a: Encryption using AES algorithm

AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using common private key, an example is shown in Figure 1a, it can be seen the cipher text should be in different from and gives no clue to the original plaintext. Figure 1a shows the Encryption of AES operation using cipher key. Where the plain text along with key is given to encryptor, which encrypt the plain text into cipher text, which is the result of encryption process. In reverse the decryption take place where the cipher text along with key is given to decryptor and it result into the original plain text as shown in Figure 1b.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

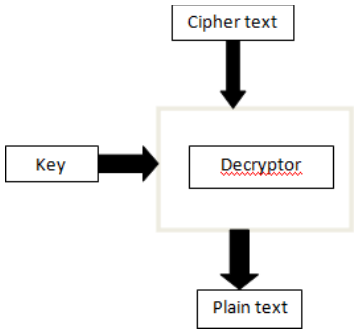


Figure 1b: Decryption using AES algorithm

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure,the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128-bit (16 bytes, 4 words), 196-bit (24 bytes, 6 words) and 256-bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

IX. RESULT

Figure 2: Home Page

Figure 3a: Selection Page

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

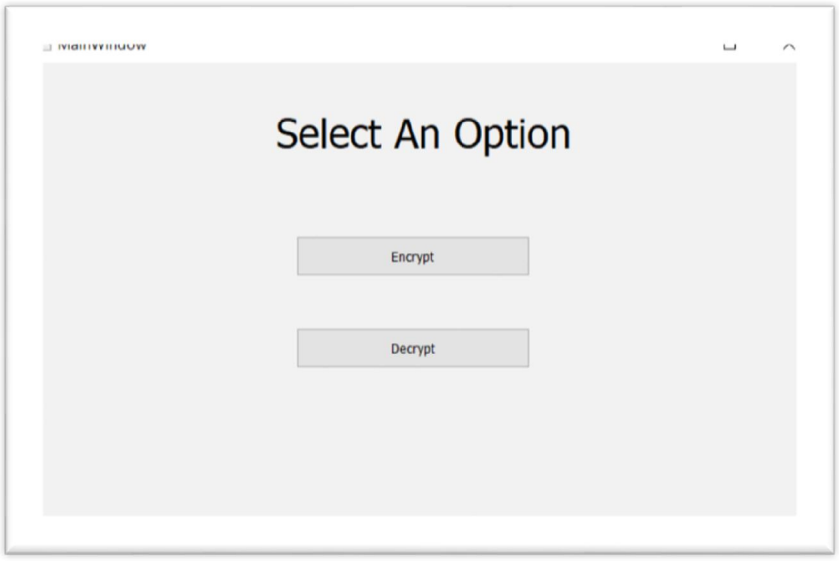


Figure 3b: Selection Page (Encrypt or Decrypt)

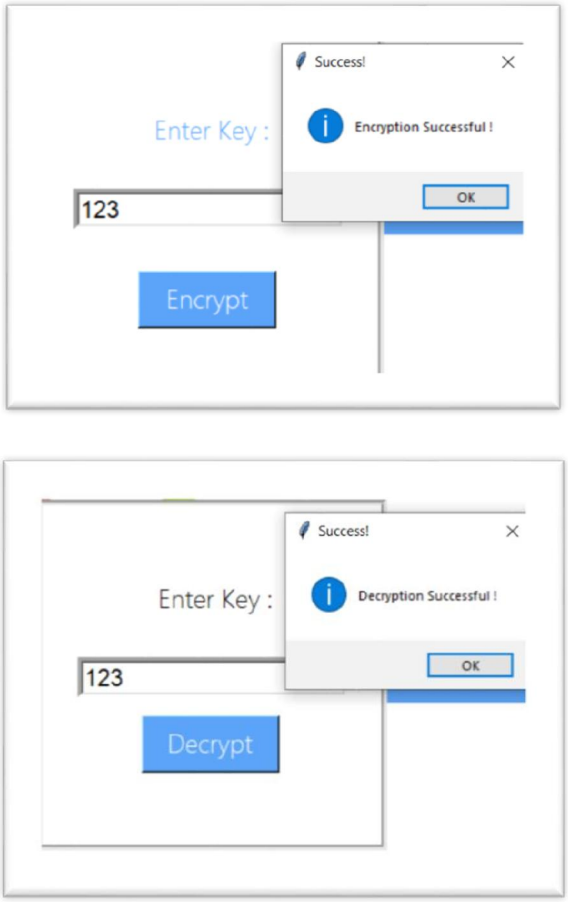


Figure 4: Result after successful Encryption and Decryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

X. CONCLUSION AND FUTURE SCOPE

In this paper we discussed that to avoid the duplication using the Encryption And decryption method. And for the text uploading we are using three algorithms., For the uploading in the cloud system we are using the Structural Similarity AES Algorithm and the main purpose of the similarity index is to check the image quality such as luminance, contrast and structure, then it measures the similarity of two image. To store large amount of data with efficiency, to avoid the duplicate text and image we are using the encryption method.

Data deduplication, an efficient approach to data reduction, has gained increasing attention and popularity in large-scale storage systems due to the explosive growth of digital data. It eliminates redundant data at the file or subfile level and identifies duplicate content by its cryptographically secure hash signature which is shown to be much more computationally efficient than the traditional compression approaches in large-scale storage systems.

REFERENCES

[1] S. Halevi. D. Hornik. B. Pinkos. and A. Shulman-Peleg. "Proofs of ownership in remote storage systems," in Proceedings of the 18th ACM SIGSAC Conference on Computer and Communications Security. ACM, 20 II, pp. 491-500.

[2] Gonzalez-Manzano and A. Orfila. "An efficient confidentiality preserving proof of ownership for deduplication," Journal of Network and Computer Applications. vol. 50, pp. 49-59, 2015.

[3] J. Blasco, R. Di Pietro, A. Orfila, and A. Sorniotti. "A tunable proof of ownership scheme for deduplication using bloom filters," in Communications and Network Security (eNS). 2014 IEEE Conference on. IEEE.

[4] W, K. Ng. Y. Wen, and H. Zhu, "Private data deduplication protocols in cloud storage," in Proceeding~ of the 27th Annual ACM Symposium on Applied Computing; ACM, 20 12, pp. 441-446.

[5] Oi Pietro and A. Sorniotti. "Boosting efficiency and security in proof of ownership for deduplication." in Proceedings of the 7th ACM Symposium on Information. Computer and Communications Security. ACM, 20 12, pp. 81-82.