IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Cloud

Prof. A. A. Pund[1], Kardile Chandrkant[2], Tormad Rohit[3], Deshmukh Yogesh[4], Waghmare Shubham[5]
Dr. Vithalrao Vikhe Patil College of Engineering Ahmednagar, Maharashtra, India

Abstract: *In this study, role re-encryption is employed in a secure role re-encryption system to minimise data leakage and deduplication (SRRS). It also looks for evidence of ownership to see whether the user is an authorised one. This is for the sake of effectiveness. The role re encryption approach involves sharing the access key for the associated authorised 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 endeavour. 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 pancard, passport, ATM card, and so on, should be stored on a single wnpc. To minimise duplication in our proposed system, we are securing the text file and picture data.*

Keywords: Java, HTML, CSS

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 utilize 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 same files 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 de duplication 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 ade-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. LITERATURE SURVEY

Chippy Jacob, Rekha V. R "SECURED AND RELIABLE FILE SHARING SYSTEM WITH DEDUPLICATION USING ERASURE CORRECTION CODE",[1], Effective
file system storage and administration is critical these days to avoid wasting the storage capacity supplied by 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 keep 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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

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 using a Reversal Correcting Code approach, even if sections of both the records are lost due to an assault on any server. As an outcome, 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 the communications sent. In this research, we implemented a mechanism for sharing secret messages by encrypting them in coloured 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 in a 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 jeopardised 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 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 must be 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.

G. Sujatha; Jeberson Retna Raj, "Digital Data Identification for Deduplication Process using Cryptographic Hashing Techniques ,[6] The cloud services system is a valuable resource for businesses and individuals who require storage space for large . Many types of digital data can be stored in the space, including photographs, photos, video, and audio. Due to the fact that internal memory can be shared by multiple users, double copies of data may exist in the storage

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

space. To check for duplicates, an adequate way to uniquely identify the digital data is necessary. There are numerous methods to define technological information. One such technique is hash-based identification. Using cryptographic hashing algorithms, each component of the data might well be uniquely identified. The hashing algorithm's distinct feature aids in data identification. In this study, we will learn about the benefits of using a cryptographic algorithm method for electronic data identification, as well as a comparison of numerous hashing algorithms.

Ying Wang; Quyuan Wang; Songtao Guo; Yuanyuan Yang, "Deduplication-Oriented Mutual-Assisted Cooperative Video Upload for Mobile Crowd Sensing
",[7] Deduplication (removing redundancy) and cooperative video distribution are two prominent methods for usage while ensuring video capture in damaged networks. However, deduplication is typically conducted on texts and photos. Furthermore, most deduplication systems necessitate global information and are distinct from video routing. To address such issues, the paper suggests a cooperative upload technique for sensing videos that achieves local video deduplication without excessive comparison and feature sharing. the spread of redundant items produced by content-free video routing, we combine content-aware deduplication with dynamic relay selection. to encourage relay cooperation and load balance, we incorporate a novel mutual-assisted mechanism into our system. The deduplication-assisted upload is modelled as a multi-stage decision issue. We create a stepwise Mutual-Assisted Video Upload Algorithm (MAVU) to schedule video chunks and eliminate duplicates the uncertainty of destinations in the choice problem. Extensive trials are being to compare MAVU against existing algorithms. The numerical findings our MAVU outperforms the other algorithms of collected video size and upload latency.

Minal Bharat Pokale; Sandeep M. Chaware, "De Duplication Approach with Enhance Security for Integrity ",[8] An essential thing of the IT-business. It offers computing tools, software, hardware, and computing resources to the user. A huge amount of people connect 1 due to the sheer comfort it provides. The user only pays for the services that he or she uses in this situation. A vast amount of data, including personal files, images, PDFs, text, and multimedia data, is now stored in the cloud. Security is one of the most pressing concerns. Everyone wants to be able to submit and save data without having to be concerned about security. It is the responsibility of the IT organisation to ensure that the data is secure. It is critical to check the integrity of documents since their content can be altered by an external attacker. This data is duplicated, wasting a lot of space. Data must be de-duplicated before being transferred to the cloud server to avoid this. This safe hashing algorithm is used. It calculates and saves the hash function for a block of data. In addition to minimising unnecessary waste of space, administrators should think about security. The document's integrity is checked using TPA. Both problems are expected to be addressed by this system.

Ashish Agarwala; Priyanka Singh; Pradeep K. Atrey, "Client Side Secure Image Deduplication Using DICE Protocol ",[9] Secured data compression has grown in prominence since the advent 1 of cloud computing. In the literature of this continuing research area, many strategies have been proposed. The Message Locked Encryption (MLE) scheme is frequently discussed among these strategies. Researchers have developed MLE-based techniques for safe data deduplication, where the data is typically in text form. 2 As a result, multimedia data such as photographs and video, which are larger than text files, have received little attention. Secured data deduplication applied to such data files could greatly reduce the cost and storage space required. We offer a safe deduplication strategy for strikingly similar (NI) images utilising the Dual Integrity Divergent Encrypt (DICE) protocol, a variation of the MLE-based scheme, in this study. The suggested approach divides a picture into blocks, and the DICE protocol 1 is applied to each block individually rather than to the full image. As a result, the blocks that are shared by two or more NI pictures are only kept once in the cloud. We present thorough assessments 2 of the proposed scheme's theoretical, experimental, and security features.

2.1 Problem Statement

To Create A System That Uses Data Deduplication To Achieve Effective Cloud Storage In Order To Avoid The Problem Of Data Redundancy.

2.2 Motivation and Need

Encrypted file deduplication schemes can enhance cloud storage space utilization while still protecting file privacy

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

III. PROPOSED SYSTEM

The working of the proposed is based on the fact that the texts present in images have some unique features which include the properties of edges. The block diagram of the proposed method is shown in Figure 2. The proposed method is mainly divided into three modules viz. Edge map generation module, Text area segmentation module and Text recognition module. The input is an image to the system and the output obtained is in the form of a text is less.

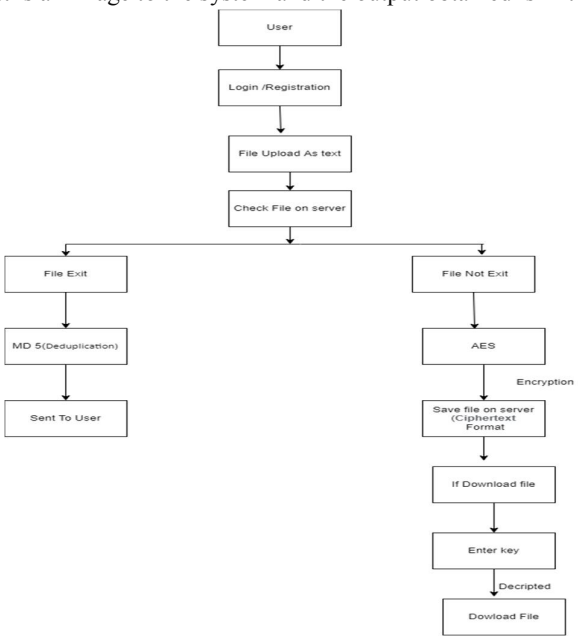

Fig.1.System Architecture

3.1 Modules

Admin

In this module, the Admin has to login by using valid user name and pass word. After login successful he can do some operations such as Upload file, Check Dedublication and Store file in encrypted format, download file in decrypted format

Upload file

In this module, the admin can upload image or text file to server.

Deduplication

For the Deduplication we use MD5 Algorithm. If deduplication Occur in file then we sent to user again and if file contain is not deduplication then store file.

Encryption

File contain is unique that time AES algorithm working and store file in encrypted format

Decryption

If a user wishes to access or download a file in its original format, the AES algorithm will do so. End User or Outcome There are n number of users present in this module. Before doing any operations, the customer must first register. When a user registers, their information is added to the database. After successfully registering, he must login using his permitted password. Once logged in, the user will indeed be able to perform activities such as uploading files, checking for de duplication, encrypting and storing files on the server, and downloading files.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

IV. EXISTING SYSTEM

In the secure role encryption system, it has worked on two encryption i.e, the convergent encryption and role encryption. The convergent encryption is used to avoid the leakage of duplicate data in the cloud system. And also it achieves the authorized duplication. Meanwhile the role encryption prevents data leakage and it checks the ownership. Then the user sends the request to the management center, and it checks for the authorized request. After responds from the management center, the user can upload the text file . When the user sends the text file for the first time it automatically uploads into the cloud server system with the help of role key generation, if again some other user or the user sends the same text file then it is not upload

Software Requirement

Java is an object-oriented programming language with a high level of abstraction and as few implementation dependencies as possible. Java is used to create applications for several platforms that run the Java Runtime Environment (JRE), as well as applications that run on a single device such as a desktop or mobile phone. Java can also be used to create distributed applications.

V. CONCLUSION

The goal of this study was to find effective strategies for dealing with respetivity motion identification in individuals. It is possible to reach a conclusion based on the analysis. We applied machine learning and provided a large amount of data to ensure correctness. Check image already store or duplicate (perform MD5)

VI. 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 the real algorithm .,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 .

VII. ACKNOWLEDGEMENT

We'd like to thank our guide Saraswati Patil, as well as the Vishwakarma Institute of Technology, for their help with this project.

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 I I, pp. 491-500.

[2]. Gonzalez- Manzano and A. Orfila. "An efficient confidentiality preselving proof of ownersh ip for deduplic,uion ," 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 Comm\U1ications 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 Proceedin~ of the 27th Annual ACM Symposium on Applied Computinr; ACM, 20 12, pp. 441-446.

[5]. R. Oi Pietro and A. Sorniotti. "Boosting efficiency and security in proof of ownership for deduplicatioll." in Proceedings of the 7th ACM Symposium on Infonnation. Computer and Communications Security. ACM,2012, pp. 81-82

[6]. M. Li. C. Qin, and P. P, C. Lee, "Cdstore; toward reliable, secure. and cost-efficient cloud storage via convergent dispersal," in Usenix Technical Conference,2015 , pp. 45-53