*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

# Role Based Secure Data Access Control for Cost Optimized Cloud Storage Using Data Fragmentation While Maintaining Data Confidentiality

**Subhash Gulabrao Rathod[1], Mangesh D. Salunke[2], Hemantkumar B. Jadhav[3], Deepika Amol Ajalkar[4], Dinesh Banurao Satre[5], Devyani Bonde[6]**

[1]Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune, Maharashtra, India;
subhashrathod@gmail.com

[2]Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune, Maharashtra, India;
salunkemangesh019@gmail.com

[3]Adsul's technical campus, Ahmednagar, Maharashtra, India;
hem3577@gmail.com

[4]G.H. Raisoni College of Engineering and Management, Pune, Maharashtra, India;
dipikus@gmail.com

[5]Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune, Maharashtra, India;
dbsatre@gmail.com

[6]Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune, Maharashtra, India;
divyabonde@gmail.com

**Abstract**— The paper proposes a role-based secure data access control framework for cost-optimized cloud storage, addressing the challenge of maintaining data security, privacy, integrity, and availability at lower cost. The proposed framework incorporates a secure authenticity scheme to protect data during storage or transfer over the cloud. The framework leverages storage cost optimization by compressing high-resolution images and fragmenting them into multiple encrypted chunks using the owner's private key. The proposed approach offers two layers of security, ensuring that only authorized users can decrypt and reconstruct data into its original format. The implementation results depicts that the proposed scheme outperforms existing systems in various aspects, making it a reliable solution for cloud service providers to enhance data security while reducing storage costs.

**Keywords**- Optimized Cloud Storage; Data Privacy; Data Compression; Data Security; Data integrity

## I. INTRODUCTION

The widespread adoption of cloud computing has revolutionized the way businesses and organizations handle data storage and management. Cloud storage provides a convenient and cost-effective solution for storing and accessing data from anywhere, at any time. However, the security of data stored in the cloud remains a major concern for businesses and cloud service providers alike. As the volume of sensitive data stored on the cloud continues to grow, ensuring the confidentiality, integrity, and availability of that data has become a top priority[1][2][3].

A traditional approach to safeguard data outsourced to the cloud is to encrypt it before uploading it. However, this approach comes with limitations as it shifts the responsibility of data protection to the security of encryption keys. As the keys gets leaked, the data becomes vulnerable to attacks. The exposure of keys may happen due to several reasons, including poor key management and bad key generation. Recent studies have focused on encryption with data splitting to overcome these limitations and enhance data confidentiality. Using secure fragmentation also enables faster and cost-effective revocation of resource access compared to traditional methods. In this paper, a novel framework is proposed that employs secure fragmentation and encryption techniques to provide a role-based secure data access control mechanism for optimizing cloud storage costs. One of the primary challenges facing cloud service providers is to provide secure data storage at a lower cost. Cost optimization is a critical factor for businesses when choosing a cloud service provider. In this context, providing secure data storage, privacy, integrity, and availability at a lower cost is a significant challenge that must be addressed. It requires a comprehensive framework that can ensure the security of data while reducing storage costs. The proposed paper introduces a role-based secure data access control framework for cost-optimized cloud storage that addresses the challenges of maintaining data security, privacy, integrity, and availability at lower cost. The proposed framework leverages a

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

secure authenticity scheme to protect data during storage or transfer over the cloud. This framework proposes a two-layer security approach that ensures only authorized users can decrypt and reconstruct data into its original format [8][9][10].

One of the significant advantages of the proposed framework is its ability to optimize storage costs by compressing high-resolution images and fragmenting them into multiple encrypted chunks using the owner's private key. Before storing data on the cloud, the proposed approach compresses the high-resolution images, reducing their storage size by up to 60% of their original size. After compressing the data, it is fragmented into multiple encrypted chunks using the owner's private key. This approach offers a highly secure storage solution, as only the authorized users who have access to the private key can decrypt and reconstruct the data into its original format. The proposed framework's two-layer security approach ensures that unauthorized users cannot access sensitive data stored on the cloud. This approach uses the role-based access control model, which grants users access to data based on their roles within the organization. This access control model ensures that only authorized users with the necessary privileges can access sensitive data.

### *A. Access control models*

In cloud computing, access control models serve as security mechanisms to manage access to resources. Various types of access control models are employed in this environment, including:

**Role-based access control (RBAC):** This is a most commonly used access control model in cloud computing is RBAC. This model involves assigning roles to users based on their job responsibilities. Users are granted access based on the roles they have been assigned [1][36].

**Attribute-based access control (ABAC):** As the name suggests the access control is totally based on a user's attributes like title, authorization level and location which is facilitated by this access control model. The attributes are evaluated against a set of policies to determine whether the user should be granted access.

**Mandatory access control (MAC):** This model is used in high-security environments where access is strictly controlled. It uses labels to determine the level of security clearance required to access a resource. Users are granted access based on the clearance level they have been assigned [2][37].

**Discretionary access control (DAC):** By implementing this access control model, the owners of resources can regulate and manage the access to their resources with ease. The resource owner determines who has access and what level of access they have. This model is commonly used in less secure environments where the resource owner has greater control over their resources.

**Rule-based access control (RBAC):** This model uses a set of rules to determine access. Access is granted based on whether the user meets the criteria defined in the rules. This model is useful in situations where access needs to be granted quickly based on specific criteria.

Each of these access control models has its own advantages and disadvantages. The choice of access control model will depend on the specific security requirements of the cloud computing environment [4][5][38]

The proposed paper introduces a comprehensive framework for cost-optimized cloud storage that addresses the challenges of maintaining data security, privacy, integrity, and availability at lower cost. The proposed framework leverages a secure authenticity scheme to protect data during storage or transfer over the cloud, and a two-layer security approach that ensures only authorized users can access sensitive data. The evaluated results shows that the proposed scheme outperforms existing systems in various aspects, making it a reliable solution for cloud service providers to enhance data security while reducing storage costs.

### *B. Contribution*

1. Advancement in storage overhead reduction, While storing the data we are compressing the data which means we are reducing the physical size of the file by 60% without compromising the quality of the data. In this case data is nothing but the images. This helps to store maximum images in a confined data storage which eventually reduces the storage cost with modified DCT-2 with threshold value compression algorithm.
2. We are providing two layers of security while storing the data, firstly data is fragmented into number of fragments and each fragment is stored separately so the attacker needs all separately stored fragments and metadata of how to join the fragments to get the original data.
3. Reconstructing images from multiple fragments, which were earlier saved by the user in the cloud, lies with the data defragmentation module. Upon receiving a request for image access from an authorized user, this module retrieves the dispersed fragments and consolidates them in the sequence indicated in the log file.
4. When conducting a data audit, we generate a signature for the user's data. The signature is created using RSA with MD5. While generating RSA keys we are padding the key with system time when user register. This additional parameter ensures that the signature is created with a

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

higher level of randomness. It ensures that even though multiple users have the same data, generated signature will be unique each time.

## II. PROBLEM STATEMENT

### *A. System Model*

We designed data access control framework for multi-authority cloud storage, as shown in figure 4.1, there are 5 entities within the framework. A certificate authority, Cloud Service provider, Data owner and data consumer, which are described as follows.

1. **Security Key Generation & Distribution** will accept the registration of all the users, it initiate the processes of generating secrete keys for the newly registered user and assigning the unique identity to the user.

2. **Admin** is responsible for approving new registered users. Grant user access to portal also admin has authority to invalidate the certificates of active users. Invalidating certificate means to revoke the user.

3. **CSP (Cloud server provider)** provides significant amount of resources for developing and maintaining cloud services. Cloud services can be anything like storage or hosting web service.

4. **Data Owner** who stores data over cloud and has to rely on cloud for computing resources. Here role of data owner is to authorise users who requested for downloading data, Owner can be both consumer of any business organization.

5. **Data consumer** can seek permission to access certain data from the data owner, and the owner grants approval, then the data user can proceed to access the requested data.

There are two processes that execute throughout the entire framework first is owner process and second is data consumer process. The owner creates the data and shares it public platform but the data consumers can only see data but not download it, this can be performed by generating the public/private key using RSA algorithm. Authorised data consumer can access the uploaded data using owner's public key.

To provide security to the data we are fragmenting data into chunks and then encrypt those chunks using asymmetric key encryption algorithm that is RSA, Owners private key will encrypt the generated chunks and owner's public key will decrypt the chunks. Here we are providing 2 layers of security by fragmenting single file into chunks and then encrypting those chunks. Our experimental results show that proposed methodology achieves high security with minimum storage cost.

### *B. Design Goals*

The implications of research based on the problem statement could be significant for several industries that generate and manage large-scale image datasets, including healthcare, satellite imaging, and military intelligence. Some potential implications of the research are:

**Improved cost efficiency**: By identifying cost-saving strategies and optimal storage solutions for large-scale image datasets, organizations could significantly reduce their storage and management costs, potentially freeing up resources for other critical activities.

**Enhanced data privacy and security**: Implementing best practices for data privacy and security in public cloud environments could help organizations protect sensitive and confidential information from unauthorized access or theft, thereby mitigating potential legal, financial, and reputational risks.

**Increased scalability**: With the exponential growth of image datasets, scalable storage solutions are becoming increasingly important. By identifying optimal storage solutions and addressing compatibility and accessibility challenges, organizations could better manage their datasets as they continue to grow.

**Improved accessibility and collaboration**: By ensuring compatibility and accessibility across different storage systems, organizations could improve collaboration and information sharing across different teams, departments, and even external stakeholders.

## III. PROPOSED SCHEME

The figure 3.1 shows how the different components of the framework work together to provide a cost-optimized and secure data storage solution. The cloud storage component would be connected to the role-based access control model, which would grant users access to the data based on their roles within the organization. The authenticity scheme, compression algorithm, and fragmentation algorithm components would work together to protect the data during storage or transfer over the cloud. Finally, the user component would be connected to the cloud storage component, allowing authorized users to access the data stored on the cloud.

**Security Key Generation and Distribution**

When a new user signs up for the system, the system generates a new set of keys through KeyGen algorithm. This process executes the RSA algorithm to produce two secret keys, namely Pukey and Prkey. These generated keys play a crucial role in the encryption and decryption of files. The owner's private key encrypts the fragments and log files

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

generated, while the public key decrypts the encrypted files. This process ensures that the files remain secure and protected from unauthorized access. With the RSA algorithm, users can be assured that their sensitive data is safeguarded against potential security breaches.

**Owners Process**

Owner has three tasks that he/she can perform in this framework upload image, approve data consumers request and view image. Image uploading task is a heavy processing task as compared to other two.

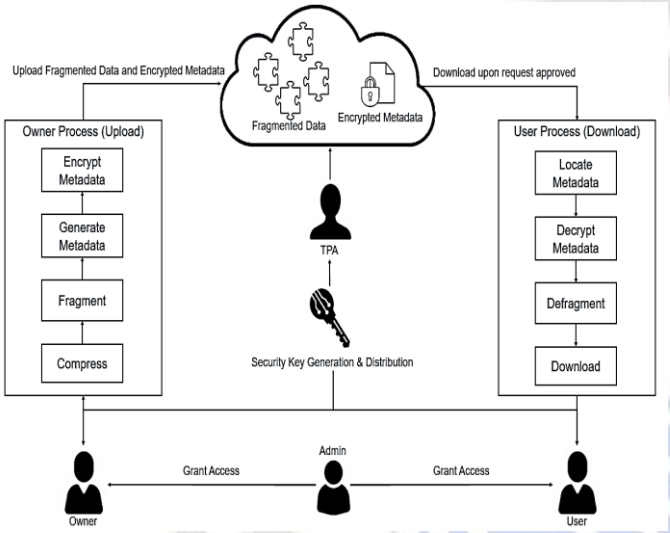


Figure 1. System model for optimized secure cloud storage

**Data Uploading**

*Compression*

This module reduces storage size by half taking pictures as input and compressing them using the DCT (Discrete Cosine Transform) algorithm [9].

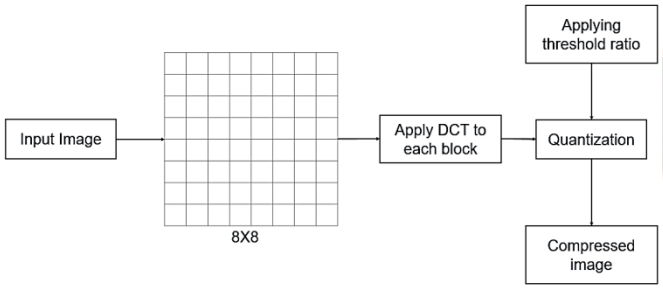


Figure 2. Data flow model for optimized compression

*Transform*

As shown in fig. 3.2 the data is transformed to decrease the redundancies between pixels in the input image. Algorithms for transform coding begin by dividing the image into smaller sub-images, typically 8 x 8 blocks. The coefficients of each block are then calculated using a transform, resulting in an array of coefficients that represent the original pixel values. The coefficients located closer to the top-left corner of the array generally contain the most information needed for quantization and encoding, while causing minimal perceptual distortion when decoded.

*Quantization*

The process of digital media compression involves quantization, where a range of values is compressed into a single quantum value. This method effectively reduces the number of symbols present in a stream, making it more compressible. To achieve this transformation, a quantization matrix is combined with a Discrete Cosine Transform (DCT) coefficient matrix. The quantization step is the main compression process, taking advantage of the fact that higher frequency components are less critical than lower frequency components. Depending on the specific quantization matrix chosen, ranging from 1 to 100, different levels of image compression and quality can be achieved. The lowest compression and poorest image quality are obtained at quality level 1, while the best quality and lowest compression are obtained at quality level 100. This enables users to select a quality-to-compression ratio that suits their needs. The standard matrix recommended by the JPEG committee has a quality level of 50. However, scalar multiplications of the standard quantization matrix can be used to obtain matrices with other quality levels. To achieve quantization, the transformed image matrix is divided by the quantization matrix, and the resulting matrix is rounded off. The values in the resultant matrix located near its upper left corner represent coefficients with lower frequencies, which are considered more significant to the human eye.

*Data Fragmentation*

The module fragments the input image into a specified number of chunks and store them over cloud, it also stores metadata about the fragmented pieces. This information contains the sequence required to reconstruct the original file. Additionally, the generated fragments are encrypted using the owner's private key, providing an extra layer of security. Even if the stored fragments are compromised, they will be unreadable and impossible to reconstruct without decryption. As a result, it would be difficult for an attacker to reconstruct the entire file even if they have access to all the chunks. This encryption process is crucial for ensuring the security of the stored data. As shown in fig. 3.3 the log file produced during the fragmentation process undergoes encryption using the RSA asymmetric encryption algorithm. The encryption is carried out

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

through the owner's private key, and decryption can be performed using the owner's public key.

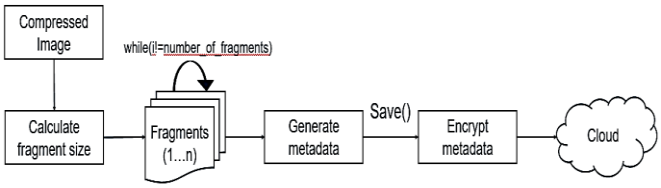


Figure 3. Data flow model for Fragmentation

**Data Downloading Phase**

*Data Defragmentation*

To rebuild an image file from encrypted fragments, the fragments must be decrypted into a readable format. During the fragmentation phase, metadata of these fragments is compiled and stored in an encrypted log file. The log file is decrypted through a log decryption process, as shown in Figure 3.4, before it is passed to the data defragmentation module. The data defragmentation module then uses the decrypted chunks and log file to restore the data to its original form. To decrypt the fragments, the public key of the data owner who uploaded the data is used.

The consolidation of the previously fragmented data pieces, stored by the owner on the cloud, is also managed by the Data Defragmentation module. Upon receiving a request for image access from an authorized user, the Data Defragmentation module locates the scattered data fragments and combines them in the order specified in the log file. This ensures that the image is restored to its original form and is available for the authorized user to access.

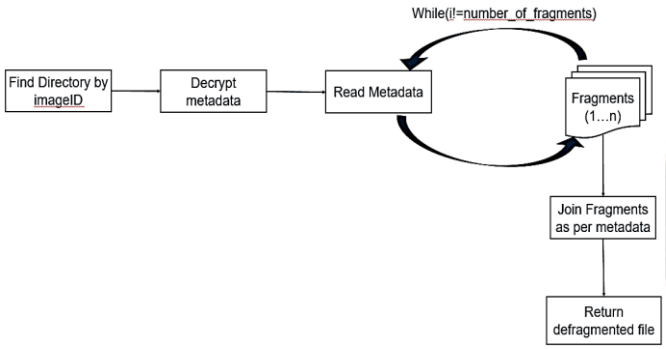


Figure 4. Data flow model for defragmentation process

**Data Auditing**

The audit procedure executes of three separate algorithms first is KeyGen which is responsible for generating asynchronous keys second is SigGen which is responsible for generating client side as well as TPA side signature and finally VerifySign which verify client side signature as well as TPA side signature and results the proof of verification.

To determine if the cloud server contains the uploaded file F, TPA sends an auditing message. Upon receiving the response message, TPA extracts the file and uses VerifySign to create a digital signature using both the data file F and the user's PuKey. TPA then verifies the digital signature to assess the data integrity of the file [8].

Our approach enables the auditor to perform data audits with enhanced efficiency. While carrying out operations, the auditor is granted read-only permissions, and the method is designed to accommodate dynamic operations. This results in a dependable cloud-based system with verified accuracy of user data, increasing its reliability. Batch auditing is also supported. We utilize RSA with MD5 to create a signature, which is then stored in the cloud. While generating a RSA key, an additional parameter is included, which is the current system time. This enhances the random probability of generating a signature. Even if a thousand users have the same data, they will all have distinct digital signatures because of the padding with the current system time which will be different on each machine when the data is saved. The system time is in milliseconds, so it is different for each person when they save it.

We aim to maintain the freshness of data during cloud system operations while minimizing storage costs. Our proposed architecture includes an effective system that helps us achieve this objective. With minimal communication, the TPA decrypts user data and creates its own digital signature. Our cloud database is protected from data modification by granting the TPA read-only privileges. It retrieves the user's public key and inputs it into the database for data decryption. It then generates its signature utilizing all of the user's characteristics and produces the final signature.

## IV. PERFORMANCE ANALYSIS

Fig. 4.1 provides information about the original size of five different images in MB as well as their corresponding compressed sizes in KB. The original size of "Image 1" is 1 MB, and it has been compressed down to 250 KB. The figure shows that as the size of the original images increases, the degree of compression achieved is relatively lower, resulting in a smaller reduction in size compared to the original size.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

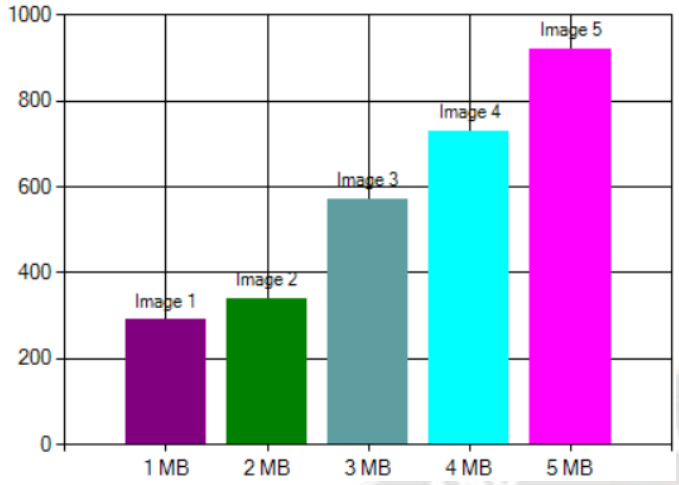


Figure 5. Storage size difference between original image and compressed image

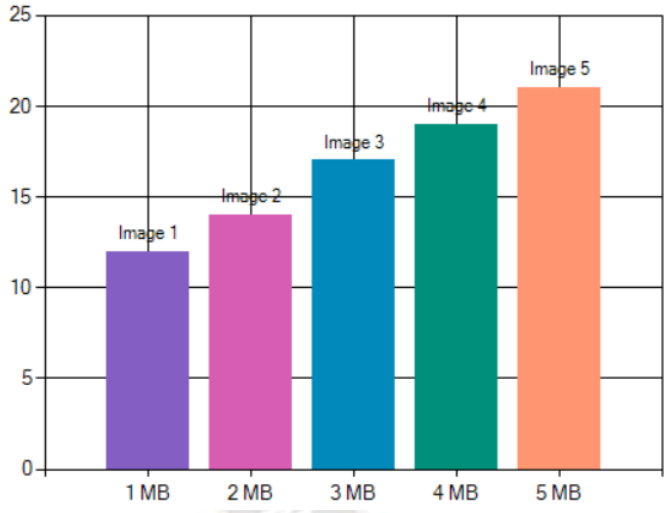


Figure 6. Owner Processing Time with variant image storage sizes

Fig. 4.1 and 4.2 shows the time difference of user process and owner process; Owner side process contains heavy operation like compression which increases the overall processing time on owner's side. Illustration 4.1 and 4.2 shows a connection of direct correlation between the enlargement of data storage capacity for images and the duration needed to handle the file of that image.

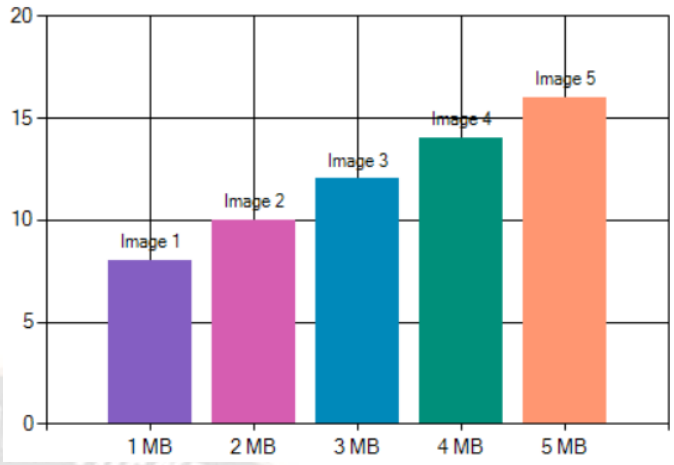


Figure 7. Owner Processing Time with variant image storage sizes

For evaluating total processing time we have considered two sides that is total processing time at owner side and total processing time at data consumer's side. Fig. 4.1 and 4.2 depicts that as image size increases its processing time also increases.

## V. CONCLUSION

The proposed framework for decentralized authority data access control is designed to share data with authorized data consumers, while allowing the data owner to revoke access rights from any data consumer at any given point. Our approach offers storage optimization and multi-layer security by fragmenting the data and encrypting it. During the fragmentation process, a single file is split into chunks, which are encrypted before being stored in the cloud. This means that even if an intruder gains unauthorized access to the stored data, they would need to decrypt the chunks in order to reconstruct the data file into its original form.

This multi-authority access control scheme provides robust data security and privacy for data shared in the cloud. It is a promising framework that can be applied in all remote storage systems, and it provides a secure and reliable solution for data sharing in cloud environments.

## REFERENCES

[1] Katarzyna KAPUSTA, Han QIU, and Gerard MEMMI LTCI, Telecom ParisTech, Paris, France "Secure Data Sharing with Fast Access Revocation through Untrusted Clouds" 978-1-7281-1542-9/19/$31.00 ©2019 IEEE.

[2] Li Li, Jiayong Liub "SecACS: Enabling lightweight secure auditable cloud storage with data dynamics" 2214-2126/© 2020 Elsevier Ltd. All rights reserved.

[3] Reyhaneh Rabaninejad, Seyyed Mahdi Sedaghat, Mohamoud Ahmadian Attari, Mohammad Reza Aref "An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over

Untrusted Cloud" K. N. Toosi University of Technology Department of Electrical Engineering Tehran, Iran, 978-1-7281-5937-9/20/$31.00 ©2020 IEEE

[4] Premlata Singh, Sushil Kr. Saroj "A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage" Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology Gorakhpur, India 978-1-7281-5197-7/20/$31.00 ©2020 IEEE

[5] Jian Wang, Kehua Wu, Chunxiao Ye, Xiaofeng Xia, Fei Ouyang ∗Colleage of Computer Science, Chongqing University, Chongqing, China "Improving Security Data Access Control for Multi-Authority Cloud Storage" 978-1-7281-4328-6/19/$31.00 ©2019 IEEE

[6] Aritra Dutta, Rajesh Bose, Swamendu Kuma Chakraborty, Sandip Roy, Haraprasad Mondal, Computational science Brainware University, Kolkata India "Data Security Mechanism for Green Cloud", IEEE 2021

[7] Ding ManJiang 1, Cao Kai 1, Wang ZengXi 2, Zhu LiPeng 3, 1. State Grid Jiangsu Tendering Co., Ltd, Nanjing, China 2. Jiangsu Electric Power Information Technology Co., Ltd, Nanjing, China 3. Global Energy Interconnection Research Institute Co., Ltd, Beijing, China, "Design of a Cloud Storage Security ncryption Algorithm for Power Bidding System", IEEE 2020

[8] Subhash Rathod; Ratnashil N. Khobragade; Vilas M. Thakare; K.H. Walse; Sushama Pawar, Sant Gadge Baba Amravati University, Amravati, Pune, Maharashtra, India, "Lightweight Auditable Secure Cloud Storage With Privacy Enabled Data Storage Optimization", IEEE 2022

[9] Subhash G.Rathod, Dr.R.N.Khobragade , Dr.V.M.Thakare Sant Gadge Baba Amravati University, Amravati, Maharashtra, India. "Model for Compress & Secure Image Storing over Public Cloud", Journal Of Electronics Information Technology Science And Management, 2022

[10] YANG Zhen, WANG Wenyu, HUANG Yongfeng, and LI Xing, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China "Privacy-Preserving Public Auditing Scheme for Data Confidentiality and Accountability in Cloud Storage" 2019 Chinese Institute of Electronics. DOI:10.1049/cje.2018.02.017 ©2019 IEEE

[11] Subhash G. Rathod, R N khobragade, Vilas Thakare, Sushama L. Pawar, "Security for Shared Data Over Public Cloud for Maintaining Privacy", Mathematical Statistician and Engineering Applications, 2022

[12] Fei Chen, Fengming Meng, Tao Xiang, Hua Dai, Jianqiang Li, Jing Qin "Towards Usable Cloud Storage Auditing" 1045-9219 (c) 2020 IEEE

[13] SI HAN, KE HAN, AND SHOUYI ZHANG Department of Science and Technology, China University of Political Science and Law, 102249 China "A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era" 2169-3536 2019 IEEE.

[14] Leyou Zhang, Yilei Cui , and Yi Mu , Senior Member, IEEE "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing" 1937-9234 © 2019 IEEE

[15] T. A. Mohanaprakash, Dr.J.Andrews Department of CSE, Sathyabama Institute of Science and Technology, Chennai 600119, Tamilnadu, India "Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm" 978-1-7281-1576-4/19/$31.00 ©2019 IEEE

[16] YE TAO, PENG XU, and HAI JIN, National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage" 10.1109/ACCESS.2019.2962600, IEEE Access

[17] Prof. Bhushan Thakre, Dr. R.M Thakre. (2017). Analysis of Modified Current Controller and its Implementation in Automotive LED. International Journal of New Practices in Management and Engineering, 6(04), 01 - 06. https://doi.org/10.17762/ijnpme.v6i04.60

[18] Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Tengfei Yang, School of Cyber Engineering, Xidian University, Xi'an 710071, China "Privacy-Preserving Data Sharing Framework for High-Accurate Outsourced Computation" 978-1-5386-8088-9/19/$31.00 ©2019 IEEE

[19] Wenxiu Ding, Member, IEEE, Rui Hu, Zheng Yan, Senior Member, IEEE, Xinren Qian, Robert H. Deng, Fellow, IEEE, Laurence T. Yang, Senior Member, IEEE, and Mianxiong Dong, Member, IEEE "An Extended Framework of Privacy-Preserving Computation with Flexible Access Control" 1932-4537 (c) 2019 IEEE

[20] HAN YU, XIUQING LU, AND ZHENKUAN PAN, College of Computer Science and Technology, Qingdao University, Qingdao 266071, China, "An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing" r 10.1109/ACCESS. 2020 IEEE

[21] Nikolaos Doukas, Oleksandr P. Markovskyi, Nikolaos G. Bardis Department of Mathematics and Engineering Science, Hellenic Military Academy, Vari – 16673, Greece "Hash function design for cloud storage data auditing" 0304-3975/© 2019 Elsevier

[22] Nureni Ayofe Azeez, Charles Van der Vyver School of Computer Science and Information Systems, Faculty of Natural and Agricultural Sciences, Vaal Triangle Campus, North-West University, South Africa. "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis" 1110-8665/2018 Production and hosting by Elsevier

[23] Jianghong Wei , Wenfen Liu, and Xuexian Hu "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage" IEEE SYSTEMS JOURNAL, VOL. 12, NO. 2, JUNE 2018

[24] Zhan Qin, Jian Weng, Yong Cui, Kui Ren, "Privacy-preserving Image Processing in the Cloud" 10.1109/MCC.2018. IEEE

[25] Kaiping Xue, Senior Member, IEEE, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage" 1556-6013 (c) 2018 IEEE

[26] Jianting Ning, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, Kaitai Liang, Member, IEEE, Lifei Wei, and Kim-Kwang Raymond Choo, Senior Member, IEEE "CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage" 1939-1374 (c) 2017 IEEE

[27] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou Department of ECE Illinois Institute of Technology , Department of ECE Worcester Polytechnic Institute "Ensuring

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7005*
***Article Received:** 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 02 June 2023*

Data Storage Security in Cloud Computing" 978-1-4244-3876-1/09/$25.00 ©2009 IEEE

[28] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE, "Toward Secure and Dependable Storage Services in Cloud Computing" 1939-1374/12/$31.00 2012 IEEE

[29] Syam Kumar P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University, Puducherry-605014, India,"An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011

[30] CONG WANG1 (Member, IEEE), BINGSHENG ZHANG2 (Member, IEEE), KUI REN2 (Senior Member, IEEE), AND JANET M. ROVEDA3 (Senior Member, IEEE) Department of Computer Science, City University of Hong Kong, Hong Kong "Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING VOL:1 NO:1 YEAR 2013

[31] Sahoo, D. K. . (2022). A Novel Method to Improve the Detection of Glaucoma Disease Using Machine Learning. Research Journal of Computer Systems and Engineering, 3(1), 67–72. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/44

[32] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013

[33] Kan Yang, Student Member, IEEE, Xiaohua Jia, Senior Member, IEEE, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 1045-9219/12/$31.00 © 2012 IEEE

[34] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014

[35] HUAQUN WANG1, 2 1 Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, "Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-health Record" 2169-3536 (c) 2018 IEEE

[36] R.Swathi, T.Subha, Associate Professor, Department of Information Technology, Sri Sairam Engineering College, Chennai, swathi.marthandan@gmail.com, subharajan@gmail.com, "ENHANCING DATA STORAGE SECURITY IN CLOUD USING CERTIFICATELESS PUBLIC AUDITING" 978-1-5090-6221-8/17/$31.00 c 2017 IEEE

[37] Nelmiawati Department of Informatics Engineering Politeknik Negeri Batam Batam, Indonesia mia@polibatam.ac.id, Wahyudi Arifandi Department of Informatics Engineering Politeknik Negeri Batam Batam, Indonesia wahyudi.arifandi@gmail.com,"A Seamless Secret Sharing Scheme Implementation for Securing Data in Public Cloud Storage Service" 978-1-5386-8066-7/18/$31.00 ©2018 IEEE

[38] S. Rathod, R. N. Khobragade, V. M. Thakare, K. H. Walse and S. Pawar, "Lightweight Auditable Secure Cloud Storage With Privacy Enabled Data Storage Optimization," 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2022, pp. 1-6, doi: 10.1109/ICBDS53701.2022.9935980.

[39] Rathod, S. G. (2022). Security for Shared Data Over Public Cloud for Maintaining Privacy. *Mathematical Statistician and Engineering Applications*, *71*(4), 7167-7173.

[40] Rathod, S., & Gupta, A. K. (2014). An Authentication and Recovery method for color Images.

[41] Salunke M. D, Kumbharkar P. B, & Kumar, P. (2021). *A Proposed Methodology to Mitigate the Ransomware Attack*. https://doi.org/10.3233/apc210173.

[42] M.D.Salunke, P.B., K., & SharmaYogesh Kumar. (2020). A Proposed Methodology to Prevent a Ransomware Attack. *International Journal of Recent Technology and Engineering (IJRTE)*, *9*(1), 2723–2725. https://doi.org/10.35940/ijrte.a2860.059120.

[43] López, M., Popović, N., Dimitrov, D., Botha, D., & Ben-David, Y. Efficient Dimensionality Reduction Techniques for High-Dimensional Data. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/145

[44] Salunke, M., Kabra, R., & Kumar, A. (2015). IRJET-Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-mea Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm. International Research Journal of Engineering and Technology. www.irjet.net