RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

# Enhancing Multi-Authority Cloud Storage Security with Identity-Based Encryption for Data Access Control

Priti Singh, Hari Om Sharan , C.S. Raghuvanshi
Faculty of Engineering and Technology, Rama University, Mandhana, Kanpur, Uttar Pradesh, India
preetirama05@gmail.com

## ABSTRACT

In today's landscape, the vulnerability of data storage on the cloud is a paramount concern for businesses and cloud research and development alike. The demand for cloud storage, driven by the need for cost-effective maintenance, has reached unprecedented levels. However, ensuring data security, privacy, integrity, and availability at a reduced cost poses a significant challenge for cloud service providers. For users to continue entrusting their data to the cloud, confidence in the service provider's security measures is imperative. With this in mind, we have developed a secure authentication scheme aimed at safeguarding data during storage and transmission across the cloud. Our framework prioritizes both data security and authenticity while optimizing storage costs. In our approach, high-resolution images, a common data type, undergo compression before storage, reducing their size to 60% of the original. Subsequently, the compressed data is fragmented into multiple chunks, each encrypted using the owner's private key. This dual-layer security strategy involves both data chunking and encryption, ensuring robust protection. Authorized users retain the ability to decrypt the data and reconstruct it to its original form, maintaining accessibility while upholding security measures. Through experimental execution, our proposed scheme demonstrates superior performance compared to existing systems across various metrics.

**Keywords:** Cloud Computing, Cloud Storage, Digital Media, Data Privacy, Data Compression, Data Security

## 1. INTRODUCTION

Cloud computing is a state of the art technology that allows users to store data from a large number of clients. It allows users to remotely store data so that the big organizations can cut the cost of implementing the storage units within the organizations which in turn reduces the financial overhead of data management. With the help of cloud services business organizations can remotely backup their data to third-party cloud storage provider, so there is no need to invest in purchasing the storage devices. Cloud service providers can take care of data maintenance and can recover data in case of hardware failure. Cloud storage is easy and cost effective but the security and privacy of data becomes major concern when it comes to sensitive data storage at third party. With the introduction of the data privacy protocols, data encryption before uploading it to public clouds becomes a widespread practice. Such processing strengthens the data privacy, also with the rapid development of digital media, large amount of digital datasets are being generated today, digital datasets domains such as satellite images, medical images dataset contains thousands of images for further researching and study. As digital media being generated on regular basis data storage cost becomes the major issue [2][5][8].

Strong eencryption methods can be used to take care of data security issue. Plain data should be encrypted before storing it over the cloud and data consumer who has authorised access to data can decrypt the data with unloaders public key. Cloud storage offer companies from various domain more agility and

enable them to store data without having the need Cloud storage is nothing but a virtual storage which is metered, scalable, cloud storage has revolutionized on how companies save their data and share with others. It allows users to store unlimited files to data centers which guarantees to be online all the time and can provide authorized access to anyone [7].

### 1.2 TYPES OF CLOUD SERVICES

Cloud storage service is the most widely used cloud computing service in the world. Cloud storage provides remote data access and storage and remote servers are responsible for managing stored data or deployed applications. For example (SaaS) software as a service provides applications to use in businesses without directly installing it on the local devices. Anyone can access their data directly with proper internet access [1][8][15].

Cloud computing offers centralize storage, memory and data processing. Some examples of cloud storages are drop box, Google drive [2].

Cloud computing service categorises as follows:

Infrastructure as a service (IaaS)

Platform as a service (PaaS)

Software as a service (SaaS)

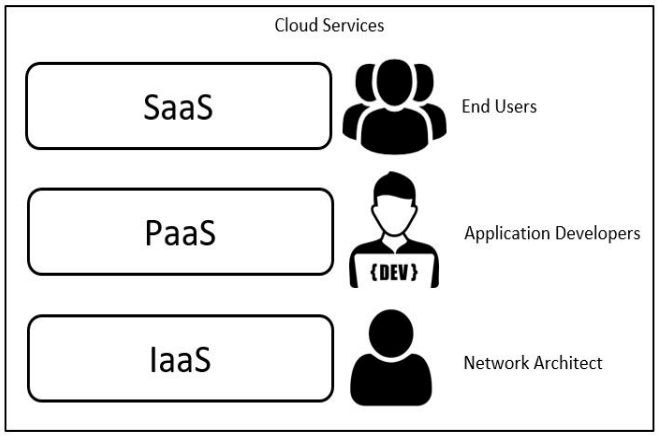


Fig. 1.1 Types of cloud services

Many organisations are outsourcing their data to cloud providers because of cost savings and ease of use. Cloud service providers provides individual services and users need to decide which type of cloud service fits the needs [10] [14].

**Infrastructure as a service (IaaS):** Private cloud storage is designed for specific individual or organisation as per their needs. Private cloud can be in house or outsource externally. Private cloud is primarily for businesses rather than individual entity. It gives full administrative access and can design system as per the business needs.

**Software as a service (SaaS):** Public cloud service gives very little administrative control. Public cloud can be accessed by anyone who is logged in. It provide security and no need to maintain the system.

**Platform as a service (PaaS):** A Hybrid cloud is an integration of private and public clouds. Like private cloud it can be customized as per the need, Sensitive data can be stored on private part of the cloud while non-sensitive data can be stored on public cloud and can be accessed by people remotely.

Depending on the need of the organization one or more services can be selected. Through data access control one can ensure data security over the cloud. However some cloud servers cannot be fully trusted so to block untrusted servers from accessing sensitive data one must encrypt data and users with appropriate authorization can decrypt data.

## 2 RELATED WORK

Cloud computing has many challenges such as data security, data backup, data storage techniques, availability. One limitation in cloud storage is user can acquire limited amount of storage as decided by the cloud service provider. Cloud service provider also has to take care of data storage space while backing up their data.

Following are the related work that worked towards data security, privacy and data access control.

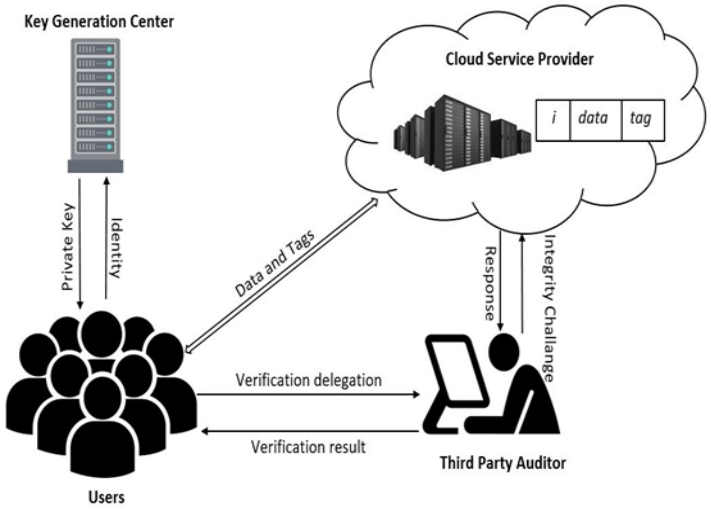


Fig. 2.1 Identity Based PDP Protocol

Author designed an architecture to securely sharing data between data owner and multiple data consumer using untrusted cloud storage. Data is processed using AON method and then fragmented and distributed over two clouds. In this way fragmented data is protected against vulnerable cloud storage providers even if one has accessed to the data, it will be incomplete, Author stated that the framework is designed in such a way that it reinforces confidentiality as well as provides simple and easy integration of access revocation using system based fragments re-encryption [1]. In gap analysis we found that the author does not used any third party auditing scheme and no work is done towards data storage optimization.

Author proposed a Secure Auditable Cloud Storage (SecACS) framework which supports data dynamics. SecACS framework takes less computation time. It uses lightweight cryptographic operations which results in framework being lightweight and takes less processing time. Upon extensive experimental evaluation author stated that SecACS data outsourcing rate is faster than previous solutions, data integrity checking is twice as faster than previous frameworks. Gap analysis shows that framework can successfully achieves data integrity but framework does not provide file encryption [2].

Focuses on the security issues while auditing the shared data. In this paper, author proposed group data sharing framework in which users who are in the sharable group can insert, update, delete separate blocks into shared data with public based ID. Besides that any misbehaving user can be blocked and can revoked any rights that the user have without any overhead. Framework is secure against public untrusted cloud servers and provide data privacy while verifying the data by public verifier. Gap analysis shows that although framework provides data integrity verification, it does not provide data encryption on cloud storage system [3].

This paper proposed public data sharing scheme where data integrity is maintained by public auditing framework by using third party auditors to assure data privacy, integrity and reliability on the cloud. For data privacy it uses 256 bit AES algorithm for encryption. For auditing it uses 512 bit secure hash and RSA algorithm for public key encryption. In terms of data operation users can perform insertion, deletion and modification of data. Gap analysis shows that the framework can provide data security, privacy and integrity but there is no provision for storage cost minimization [4].

### 2.2 SIMILAR FRAMEWORKS

**Identity Based PDP Protocol**

This protocol is mainly build to provide privacy for multiple users. It is designed to protect identity of users. TPA is responsible for auditing user's data but while auditing TPA cannot figure out the owner of the data.

There are four types of entities in this framework: key generation center, CSP, users and TPA.

(1) Key generation center generates private keys for all users subscribed to the cloud. Here author assumed that the keys are transmitted by secure channel.

(2) Cloud Service Provider (CSP) generates proofs for data integrity and maintains user's data.

(3) Users those are subscribed to the cloud creates separate tags for their data and outsource the data to Cloud Service Provider. All users are allowed to share their data in group.

(4) TPA checks the integrity of data. For auditing the data TPA sends integrity challenge to cloud service provider if TPA gets proof from CSP then only TPA can validates the proof and generate reports of data validation.

Proposed framework ensures relationship between data and data uploader in proof generation phase and not in integrity audition phase so that auditor does not know the data owner. In this paper author took efforts to protect privacy of data uploader [1][4][10][15].

### Key Aggregation Encryption And ABE Technology

Author, Huang Nana, Yang Yuanyuan proposed HealthCare cloud architecture which integrates multiple application based on privacy protection. Proposed framework uses attribute based encryption to encrypt Personal Health Record (PHR) files. Instead of traditional domain division which has public domain (PUD) and personal domain (PSD), the public domain (PUD) is further segregated into PUD1 and PUD2 is based on different access control over PHR files. Users in PUD1 has full privileges that is they can read or write PHR files, Users in PUD2 have only reading privileges [2]. In the PSD, author used key aggregation encryption (KAE) to gain read access permission. For PHR users of PUD1 and PUD2, the outsourcable ABE technology is adopted to greatly reduce the computing burden of users [2].

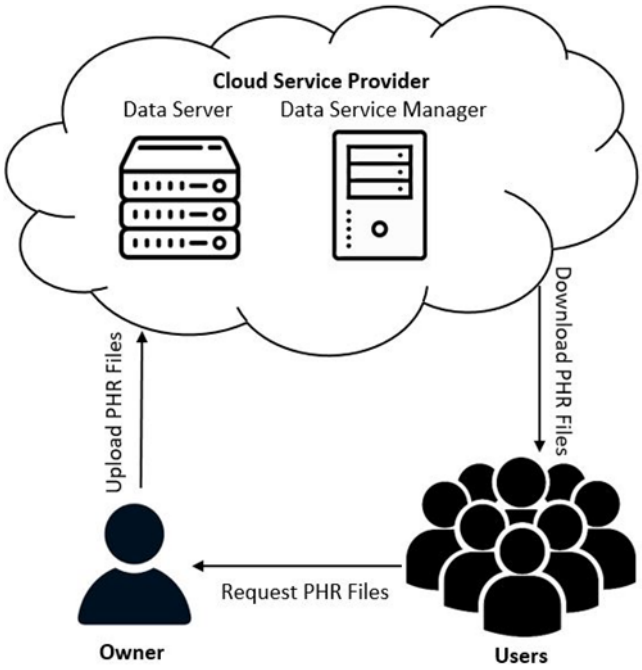


Fig. 2.2 Key Aggregation Encryption and ABE Technology

## 3 GOALS AND OBJECTIVES

Work mainly focuses on achieving following goals:

- Advancement storage optimization and low cost storage
- Secure data storage and transfer
- Authorization for stored data and access control

Objective is to ensure the data security in cloud using following methods:

- Data fragmentation and generating fragmented chunks
- Creating automated log file that holds the sequence of fragmented chunks
- Encryption of generated fragments by using asymmetric key encryption algorithm.
- Maintaining data access control.
- Minimizing storage cost using data compression techniques

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.

## 4. PROPOSED SCHEME

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. **The Certificate Authority** 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. Admin also 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 request data owner to give permission to access the data, if data owner approves it then data user can access that 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.

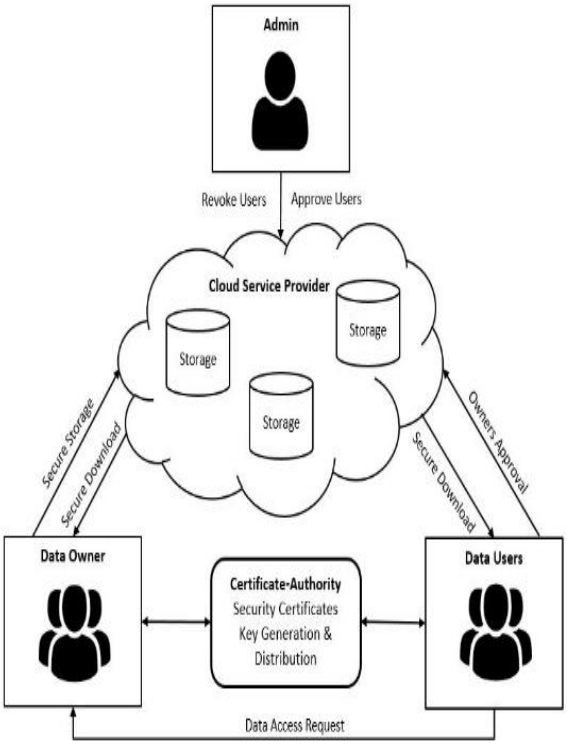


Fig. 4.1 Proposed Framework Design

**Certificate Authority Process**

When new user sign up in the system it generates new set of keys by executing KeyGen. KeyGen generates two secrete keys Pukey and Prkey, to generate these keys we are using RSA algorithm. These generated keys are then used for encryption and decryption. Owner's private key will used to encrypt the generated fragments and log file and public key will decrypt the encrypted files.

**Algorithm: Asymmetric *Key Generation***
**Input:** *int keybitsize*
**Output:** *Byte prkey, Byte pukey*
**Step 1**. ***Let*** key_instance = AsymmetricKeyPairGenerator(RSA);
**Step 2**. ***Let*** random_num = SecureRandomNumGen ("SHA1PRNG","SUN");
**Step 3**. random_num.setSeed( System.currentTimeMillisecond());
**Step 4**. generator.initialize(keyBitSize, randomAlg);
**Step 5**. ***return*** generator.generateAsymmetricKeyPair();

**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.

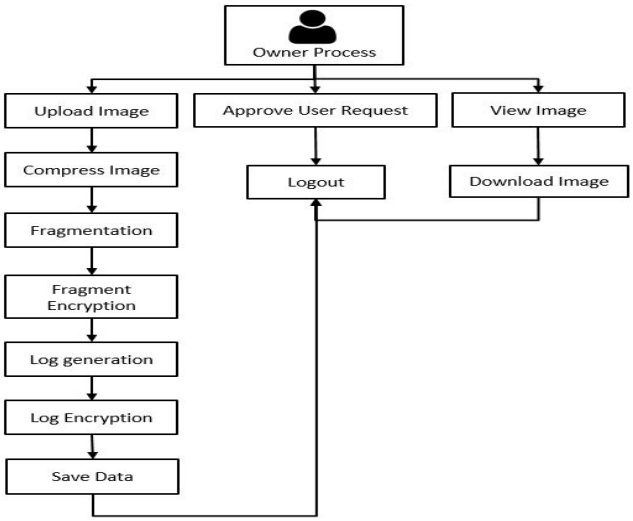


Fig. 4.2 Owners Process

**Data Uploading Phase**

*Compression*

This module reduces storage size by half taking pictures as input and compressing them using the DCT (Discrete Cosine Transform) algorithm. We use DCT because the DCT is easy to calculate and is fragmented (you can make different DCTs of rows and columns) and has "power integration" properties.

*Data Fragmentation*

This module is responsible for fragmenting input image into specified number of pieces and storing it over cloud, after fragmenting the file information about fragmented pieces is stored in log (metadata) file, information is nothing but the sequence of how to join the pieces and reconstruct the file.

*Fragment Encryption*

Here the generated fragments gets encrypted by owner's private key. Encryption is our second layer of security. Even if the fragments stored in cloud gets compromised it will not be in readable format and impossible to reconstruct it into original form without decrypting it which makes it difficult for attacker to reconstruct the entire file even if he/she has the access of all chunks.

*Log Encryption*

The log file generated during fragmentation process is encrypted using asymmetric encryption algorithm that is RSA. Here log file gets encrypted by owners private key and can be decrypted by owners public key.

**Algorithm:** ***Image Uploading (Owners Process)***
**Input:** *byte image*
**Output:** *byte[] subchunk, byte logfile.txt*
Step 1. ***Let*** byte image
Step 2. ***Let*** i_encoder = GetEncoder(ImageFormat.Jpeg);
Step 3. ***Let*** byte image' = i_encoder.Compress(Image, QF)
Step 4. ***Let*** int image_size = image'.length
Step 5. byte[] subchunk = image_size / number_of_fragments
Step 6. ***Let*** prkey = GetKey(OwnerEmailID)
Step 7. ***foreach*** fs ***in*** subchunk
Step 8. Cipher cipher = Cipher.getInstance(RSA)
Step 9. cipher.init(Cipher.ENCRYPT_MODE, prkey)
Step 10. byte cipherBytes = cipher.doFinal(fs);
Step 11. Save cipherBytes
Step 12. BufferWrite(cipherBytes.getName(), logfile.txt)
Step 13. ***End foreach***
Step 14. ***Let*** byte plaintext = Read(logfile.txt)
Step 15. Cipher cipher = Cipher.getInstance(RSA)
Step 16. cipher.init(Cipher.ENCRYPT_MODE, prkey)
Step 17. ***Let*** byte ciphertext = cipher.doFinal(plaintext);
Step 18. Save subchunk[] in log file

**Data Downloading Phase**

*Log Decryption*

Before rebuilding an image file we need a sequence of fragments. Information about fragments are compiled and saved in log file which was encrypted during fragmentation phase. Log decryption therefore decrypt the encrypted log file which is then passed to data defragmentation module.

*Data Fragment Decryption*

To reconstruct image into original form from encrypted fragmented chunks, it needs to convert into readable format by decrypting them. These decrypted chunks and decrypted log file will then passed to data defragmentation module in order to reconstruct data into its original form. Here public key of data owner who originally uploaded data is used to decrypt the fragments.

*Data Defragmentation*

Data Defragmentation module is responsible for reconstructing images from different pieces previously stored by owner onto the cloud. When authorized user request to access image this module find the location of the fragmented pieces and merge them as per the sequence in log file.

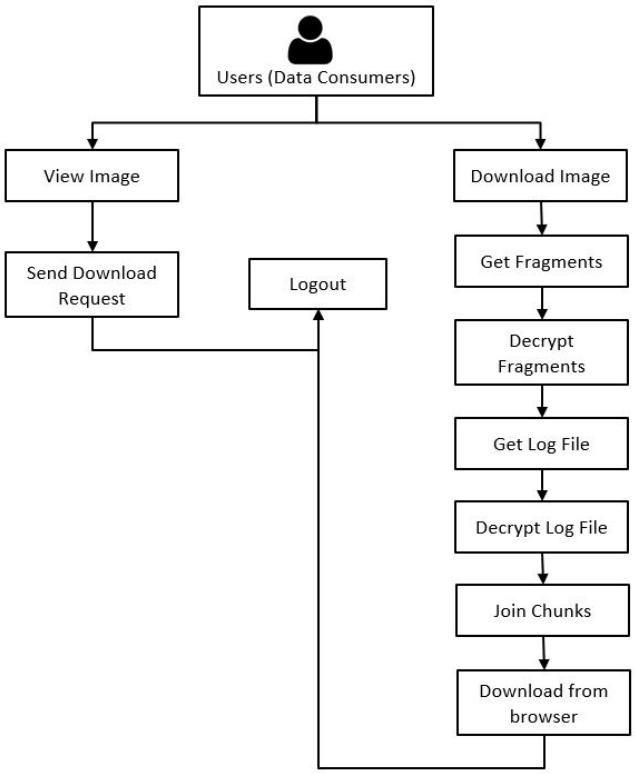


Fig. 4.3 Users Process

**Algorithm:** ***Image Downloading (Users Process)***
**Input:** *int image_id*
**Output:** *byte image*
Step 1. ***Let*** string path = getLogFilePath(image_id)
Step 2. ***Let*** ciphertext = read(path)
Step 3. ***Let*** pukey = GetKey(OwnerEmailID)
Step 4. Cipher cipher = Cipher.getInstance(RSA);
Step 5. cipher.init(Cipher.DECRYPT_MODE, pukey);
Step 6. plaintext = cipher.doFinal(ciphertext);
Step 8. Cipher cipher = Cipher.getInstance(RSA)
Step 9. cipher.init(Cipher.ENCRYPT_MODE, key)
Step 10. ***foreach*** fs ***in*** subchunk
Step 11. byte temp = Read(fs[index])
Step 12. ***End foreach***
Step 13. byte image = BufferWrite(temp)

Step 14. OutputStream output = response.getOutputStream();
Step 15. output.write(document_content);
Step 16. output.close();

## 5. PERFORMANCE ANALYSIS

For image compression implementation we can use any dataset like ImageNet which is a subset of Kaggle dataset, we do not need label dataset as we are not doing any object detection here, we are only reducing current image physical size by more than 50% without visually reducing image quality.
We are using lossy compression, considering the image size more than 5 MB most of our images will be in JPEG format so we are using Transform Coding which is a most commonly used method for compression. Initially we were considering two standard compression methods either DCT or DFT but at the end we zeroed down to DCT reasons are given below.
DCT is preferred over DFT in image compression algorithms like JPEG because DCT is a real transform which results in a single real number per data point. In contrast, a DFT results in a complex number which requires double the memory for storage. DCT is simpler and faster than DFT.
Discrete Cosine Transform (DCT) – The most widely used form of lossy compression. It is a type of Fourier-related transform, The DCT is sometimes referred to as "DCT-II" in the context of a family of discrete cosine transforms (see discrete cosine transform). It is generally the most efficient form of image compression.
DCT with Quality Factor
we did not used plain DCT rather we edited existing algorithm and added Quality Factor because we need to control the quality of the image and by compressing image with certain quality factor is way to make sure we are not losing image quality. Fig 5 shows the difference between storage sizes of original image and storage size of compressed image. Compression results shows that we have succeeded to reduce image size by more than 50% of original size. As depicted above 4 MB image when compressed does not go beyond 1 MB

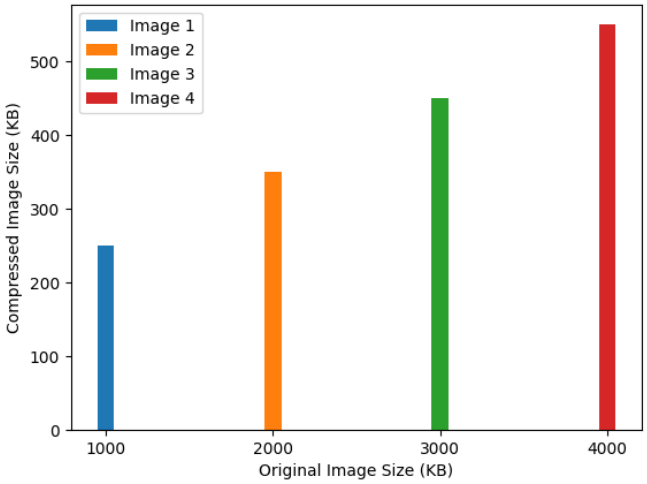


Fig. 5.1 Storage size difference between original image and compressed image

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. 5.2 and 5.3 depicts that as image size increases its processing time also increases.

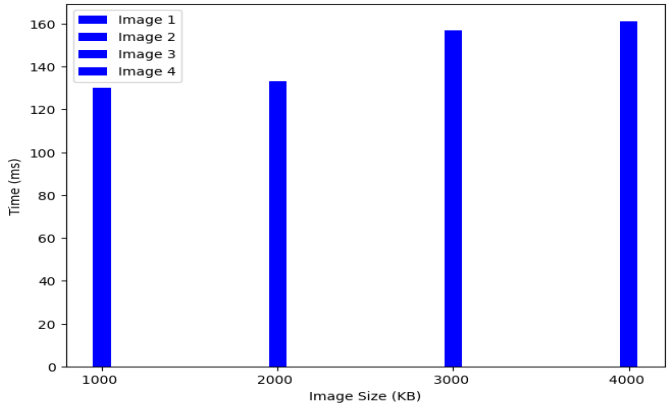


Fig. 5.2 processing time at owner's side for variable image size

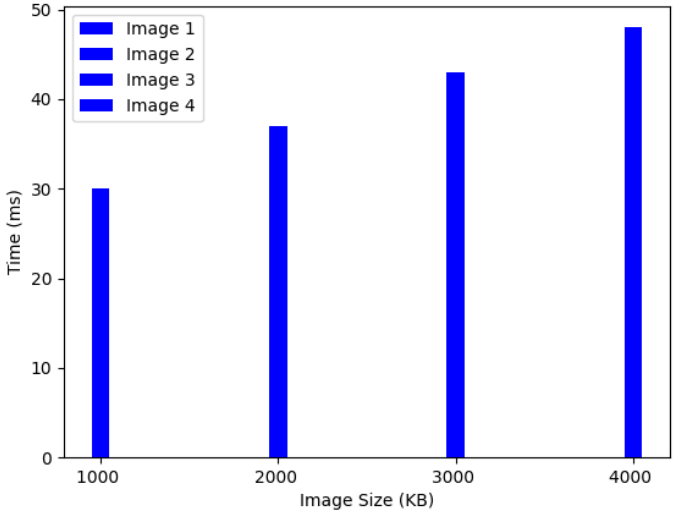


Fig. 5.3 processing time at user's side for variable image size

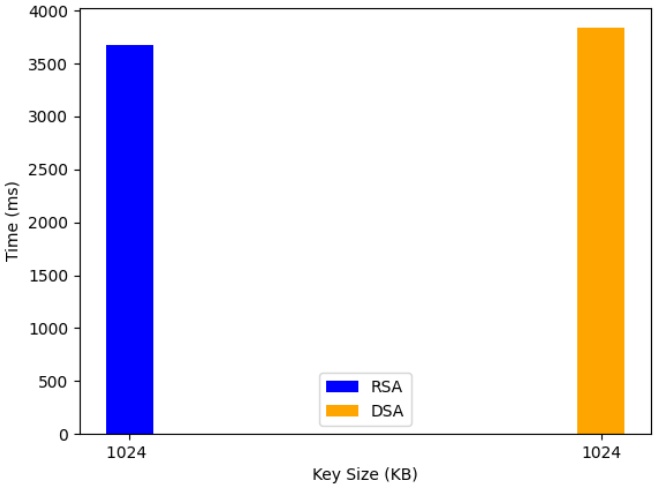


Fig. 5.4 Computation time required for Key generation by RSA and DSA

| Parameters | RSA | DSA |
|---|---|---|
| **Key Size** | Maximum key size can be 4096 bits and minimum key size can be up to 1024 bits. Size of key can be adjusted as per the need. | In DSA the standard key size is only 1024 bits and cannot be adjusted |
| **Security** | In terms of security RSA encryption is well-regarded. It is considered strong security algorithm. | DSA is not considered strong security algorithm anymore, It can leak private key while generating signature. |
| **Usage** | RSA is used for both encryption and generating digital signatures | DSA is only used for generating digital signature |

We have chosen RSA algorithm for key generation because it is stronger than DSA and supported everywhere. RSA is considered quite secure. Other than that as shown in fig. 7 it requires less computational time as compared to DSA for secure key generation.

## CONCLUSION

The conceptualized decentralized data access control framework is crafted to facilitate authorized data sharing among designated data consumers, offering data owners the ability to revoke access privileges from any consumer at their discretion. Our proposed methodology not only prioritizes storage optimization but also integrates multi-layer security protocols. Through data fragmentation followed by encryption, a single file undergoes segmentation into smaller, encrypted chunks upon storage in the cloud. Consequently, unauthorized intruders are compelled to decrypt these chunks to reconstruct the original data file, enhancing security measures.This multi-authority access control scheme presents a robust solution for ensuring data security and privacy in cloud-based data sharing scenarios. Its versatility renders it applicable across various remote storage systems, marking it as a promising framework in the realm of data management and security.

## 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] 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

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

[10] 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.

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

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

[21] 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

[22] 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

[23] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou Department of ECE Illinois Institute of Technology , Department of ECE Worcester Polytechnic Institute "Ensuring Data Storage Security in Cloud Computing" 978-1-4244-3876-1/09/$25.00 ©2009 IEEE

[24] 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

[25] 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

[26] 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

[27] 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

[28] 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

[29] 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

[30] 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

[31] 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

[32] 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