ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 1, Issue 11, DOI: 10.29027/IJIRASE.v1.i11.2018.209-215, May 2018

A Secure Cloud Media Center Application with Secure Deduplication and Anticollusion Attack Using Saaa Model

S.Alamelu [1] , Dr. A.Akila [2]
[1] *M.Phil Scholar, Department of School of computing Sciences, Vels Institute of Science,Technology &Advanced studies , Chennai, Tamilnadu, India*
[2]*Assistant Professor, Department of School of computing Sciences, Vels Institute of Science,Technology & Advanced studies, Chennai, Tamilnadu, India*
gsubalamu@yahoo.com, akila.scs@velsuniv.ac.in

Abstract— In cloud computing, clients can impart information among gather individuals to the characters of less upkeep and little administration cost. Sharing data must have security guarantees, if they are out sourced. Sharing data while giving assurance shielding is so far a testing issue, when change of the investment. It might cause to the interest strike for an unsecured cloud. For existing procedure, security of key development depends upon the shielded correspondence channel, in any case, to have such channel is a solid supposition and is troublesome for getting ready. We propose a secured data sharing arrangement for dynamic customers. Key apportionment stayed away from with no protected correspondence diverts and in this way the customer will get the individual key from accumulate director. Data deduplication is one of the methodologies which used to handle the emphasis of data. Our proposed structure keeps the replication of records and media report like pictures, accounts. The deduplication procedures are customarily utilized as a part of the cloud server for decreasing the domain of the server. To keep the unapproved use of data getting to and make duplicate data on cloud the encryption strategy to scramble the data previously set away on cloud server. CloudMe is proposed for distributed storage. All records of information proprietors are scrambled utilizing AES(Advanced Encryption Standard) calculation and put away in genuine cloud. In this manner we exhibit a safe framework engineering plan as our underlying exertion towards this course, which connects together the progressions of video coding methods and secure deduplication. Our plan empowers the cloud with the vital deduplication usefulness to totally dispose of the additional capacity and transfer speed cost.

Keywords*-cloud, security; privacy; collusion attack; deduplication*

I. INTRODUCTION

Clodu computing is the most requested propelled innovation all through the world. It is a standout amongst the most huge point whose application is being investigated in the present time. Distributed computing is relate inventive innovation that is upsetting the methods we tend to do processing. The key idea of distributed computing is that you simply don't purchase the equipment, or maybe the PC code, you might want any more, rather you lease some procedure control, stockpiling, databases, and some other asset you might want by a provider for each a compensation as-you-go demonstrate, making your venture littler and bound to activities rather than to resources obtaining. Cloud isn't just the most recent term for the Internet, however the Internet is an essential establishment for the cloud, the cloud is something more than the Internet. The distributed computing gives better administration, minimal effort, adaptable, flexibility, transportability, versatility and accessibility(anytime, anyplace and all around). Eventhough clients and merchants unverifiable with the security issues like secrecy, protection, verification, approval and information respectability. In any case, security concerns transform into the rule impediment as we now outsource the limit of data. To ensure data security, mystery and uprightness, an ordinary approach is to scramble data records before move the data into the cloud. Out of the blue, it is hard to outline an ensured and intense information sharing course of action, expecially for dynamic social events in the cloud. This paper bases on information encryption and secure information sharing schem, which can accomplish secure key portion and information sharing for dynamic social event.

Arul Jothy et al. [19] displayed two systems to be specific information encryption and document part are utilized. For document encryption utilized AES(Advanced Encryption Standard) and PGP(Pretty Good Privacy) calculation. At first when client transfers a document, it is encoded utilizing AES encryption calculation and again information is scrambled utilizing PGP calculation to enhance the system security. At that point that encoded document is part into level with segments per the measure of mists and kept in multicloud

Vishal et al.[14] exhibited Advanced encoding standard is regularly utilized encoding algorithmic program, it's bolstered numerous substitutions, change and change. Starting at these days, no practicable attack against AES exists. Along these lines, AES is most popular encoding standard for governments, banks and high security systems around the world. AES algorithmic program possess less memory than Blowfish calculation. AES calculation is a profoundly secure encryption technique. It is ensure against an assortment of assaults, for example, square assault, key assault, key recuperation assault, future assault, crush assault and differential assault.

Aarti et al.[6] developed an edge middle person re-encrytion design and annihilation codes over illustrations. The edge go-between re-encryption subject supports scrambling, encoding and sending. By abuse the edge middle person re-encryption subject, they introduced an ensured circulated capacity

system that gives secure data accumulating and secure information sending to the cloud.

Aarti et al.[6] developed an edge middle person re-encrytion design and destruction codes over illustrations. The edge middle person re-encryption point supports scrambling, encoding and sending. By misuse the edge mediator re-encryption subject, they displayed an ensured conveyed capacity system that gives secure data storing and secure information sending to the cloud.

This paper is one of a development of articles that towards decreasing information hoarding utilization. Regardless, these days more volumes of informational collection away at remote cloud servers. Among these remote set away chronicles, the greater part of them are reproduced: as indicated by yuan et al.[9] assessed 75% of information is copied. This advancement called to be specific deduplication, in which the cloud servers may need to deduplicate by keeping just a particular duplicate for each document and make a relationship with the record for each customer who claims or requests to store a near report.

Ghemawat et al. [1] authorized data dividing way to deal with help the dependableness, handiness and data get to execution inside the capacity framework, inside which the underlying data is hang on inside the kind of data pieces of steady size. Albeit, instead of taking the variable circle disappointment rate examples of capacity gadgets into thought, these investigations conjointly consider the disappointment rates of the capacity gadgets as a simple steady cost.

Pinherio et al.[2] outlined the circle disappointment rate design inside the IDEMA vogue, inside which isolates the time of plates into particular life stages with unmistakable circle disappointment rates, and conjointly direct their examination bolstered the plate disappointment rates gave by IDEMA guidelines and Google's nine-month plate disappointment slant contemplate.

Whatever is left of the paper is dealt with as takes after. The related work on data assurance, data sharing, information duplication, information stockpiling and savvy is tended to in segment II. The proposed demonstrate is expressed in area III. Our SAAA demonstrate usage is displayed in detail in area IV, trailed by the security examination and execution assessment in segment V separately. At long last, the conclusion is made in segment VI**.**

II. LITERATURE SURVEY

We quickly review to ensure data security. A common approach is to encode data reports using AES count, key dispersal and data sharing arrangement for dynamic get-togethers and Secure deduplication.

In Comparative Analysis of AES and DES security Algorithms, Sumitra [4] Presented AES encryption calculation is utilized to give security in distributed computing since encryption and decoding time taken by AES is least when contrasted with others. So it is quickest piece figure calculation among all dissected figure calculations, for example, blowfish, DES, triple DES.

In the paper entitled Architecture for Data Security in Multicloud Using AES-256 Encryption Algorithm, Rashmi et al.[11] arranged new outline for improving the data security in multicloud upheld 2 instruments information encoding and record cacophonic. AES-256 encoding principle is utilized for encoding, at that point that scrambled record is splitted into three equivalent scope of segments and keep into multicloud. AES-256 control is more secure than elective symmetrical encoding calculations. It furthermore defends documents from programmers in review entire record.

In A Secure Anti-Collusion data Sharing topic for Dynamic groups inside the Cloud is proposed by Zhongma Zhu et al.[13].They arranged secure methods for key appropriation. Clients will immovably get their own keys from bunch administrator, their topic can do fine-grained get to administration. They'll shield the subject from conspiracy assault. The arranged topic contains framework information designing, client enrollment for existing client, document transfer, client disavowal, enlistment for fresh out of the box new client and record download.

In Secure multi proprietor information sharing for dynamic gatherings in the cloud, Liu et al.[7] arranged topic named mona. That is named a safe multi-proprietor data sharing subject. This subject arranged to do fine-grained get to association and revoked clients won't be able to get to the sharing adjusting again once they're denied. Anyway, this subject could encounter the evil impacts of plot attack by the denied customer and moreover the cloud.

In the paper entitled Achieveing secure rolle-construct get to control in light of scrambled information in distributed storage is proposed by Zhou et al.[8] Presented a plan that can do secure enormous data stockpiling inside the cloud with temperate client repudiation that blends part based access administration strategies and cryptography. This plan basically experience the ill effects of arrangement assaults. At last, this assault will cause uncovering delicate data documents.

In High secure and check instrument for distributed storage, Lukka Ramesh Babu and Vemu Tulasi [10] proposed new idea for putting away and recovering the information to look after respectability. They presented new ideas, for example, finding the resultant estimation of information obstruct by utilizing calculations, for example, (keygeneration, signature age, Generation verification and Verify evidence) and that will be put away at TPA(third party inspector) and customer. To ensure that TPA cann't see any factor in regards to the first data keep inside the cloud server all through the conservative examining strategy. In existing framework accessible just for private cloud in one way however this framework has a place with

1. Legitimately not keep information from outside gatherings amid the evaluating.

2.Data spillage still remains an issue

3. It isn't a constant answer for information confirmation when the information is download. However, in the proposed framework its giving algorithms(for putting away the information and recovering the information) for both confirmation and security. In proposed framework TPA can deal with various review sessions shape diverse clients for their outsourced information, which used to give better outcomes to more secure and profoundly proficient.

In Secure Role-Based Access Control on Encrypted Data in Cloud Storage utilizing Raspberry PI, Rohini Vidhate et al. [12] showed part based encryption scheme(RBE) that facilitates the crytographic systems with RBAC(Roll Based Access Control). anticipated RBE subject, they built up an outline utilizing a cross breed cloud foundation for secure cloud data sorage. This engineering might be a composite of individual and open cloud, wherever the individual cloud is utilized to store exclusively the associations' touchy data, and along these lines the general population cloud is utilized to store the specific data that is inside the encoded kind.

In Developing Framework For Secure Storage In Cloud Computing System, Rohit Bajaj [5] proposed customers data zone unit hang on solidly by keeping up the classification and honesty of the information at interims the cloud. This method gives an answer by exploitation reliable stage module. Relate recorded arrangement framework is utilized to scramble the client's data. This procedure improves data security against a PC client inside the cloud.

In the paper entitled Towards Encrypted Cloud Media Center with Secure Deduplication, Yifeng Zheng et al. [18] presented flexible video coding strategies and secure deduplication. The deduplication presence of mind to totally take out the additional amassing and information measure cost. Specifically, it supports secure deduplication with strong video protection against harmful customers, disengaged brute force ambushes and untrusted cloud. This paper concerned framework system incorporate 3 stages: starting transfer, succession transfer and video recovery.

Ensuring Cloud Data Reliability with Minimum Replication by Proactive Replica Checking. Wenhao Li et al. [15] proposed a regard fruitful information dependableness organization segment name PRCR maintained a summed up information dependableness show. PRCR can lessen from 33% to 66% of the distributed storage space utilization and significantly bringing down the capacity esteem in an exceedingly cloud. This paper presents 3 noteworthy commitments.

1. A summed up display for muiple imitations is arranged with variable plate disappointment rates is all around examined.

2. To limit the capacity utilization and capacity cost.

3. As an immediately outcome of PRCR, the base replication benchmark with any data dependableness request are frequently given.

Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage. Junbeom Hur et al. [17] Implemented an absolutely fascinating server-side deduplication plot for encoded data, that extended a fine-grained possession organization in appropriated capacity for secure and reasonable deduplication. decisions of this arrangement may be a reencryption framework that licenses dynamic updates upon any possession changes inside the appropriated stockpiling. This plan accomplishes learning security and secrecy inside the distributed storage.

A Light-weight Data Replication for Cloud Data Centers Environment. Mohamed et al. [3] created replication procedure to improve the accessibility of the framework. This paper explored following focuses, accessibility and proficient access of each record in the server farm, and concentrated an approach to enhance the reliableness of the information documents. Likewise arranged versatile system distinguishes the best replication area utilizing heuristic scan for the best replication issue of each record.

III. PROPOSED MODEL- SAAA(Subramaniyan Alamelu Akila Ananth) MODEL

A. Architecture of Proposed Model

Architecture of proposed demonstrate comprises of Admin, Group memebers or gathering client and Cloud.

Supervisor or Group executive acknowledges responsibility of structure parameters age, client determination, and client revocation. In the sensible applications, the get-together official when in doubt is the pioneer of the social affair. Along these lines, we recognize that the get-together manager is completely trusted by trade social affairs.

Social affair people (customers) are a game plan of enrolled customers that will store their own particular information into the cloud and offer them with others. In the game plan, the social gathering collaboration is progressively changed, when the new client enrollment and client repudiation.

Once the client is repudiated, the gathering chief makes the new encryption key for the particular gathering and transmits in a scrambled arrangement. Second the gathering trough refreshes the entire information list in the cloud server. Third the gathering supervisor refreshes the client list and actuates the key for get to.

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 1, Issue 11, DOI: 10.29027/IJIRASE.v1.i11.2018.209-215, May 2018

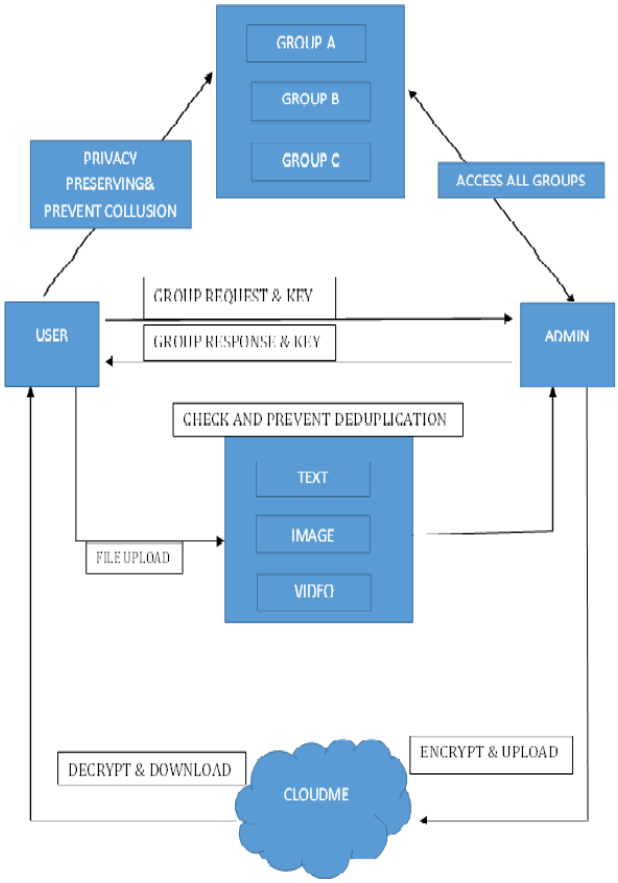

Fig 1. Illustration of SAAA - Architecture Model.

Procedure for the group member or user to upload a files such as text, image and video.

Step 1: It will check the reduntant data using SHA1(Secure Hash Algorithm1), SHA2(Secure Hash Algorithm2) algorithm and SVC technique.

Step 2: If the content of file is not existing then the file will sent to Group manager, otherwise it will display file already existing.

Step 3: File will be encrypt using AES Encryption algorithm and then it will send to cloudme storage.

Group member try to download and decrypt the file

Step 1:Group member or user send file request to group manager

Step 2: group manager will send response with decrypt key to group user, then user can download and decrypt the file.

B. Goals of the Proposed System

The fundamental objectives of the proposed plot including information protection, key dissemination, get to control, effectiveness and secure deduplication are depicted beneath.

Data privacy: Information security requires that unapproved customers are unequipped for taking in the substance of the set away data. To keep up the responsiveness of data security for dynamic parties is 'in the not very removed past a fundamental and testing issue. Especially repudiated customers can't unscramble the set away data record after the debate.

Key distribution: Key task is that customer can safely get their private keys from the head or gathering manager. In other existing plans, private key dissipating depends upon the shielded correspondence channel, however , in our course of action, we can accomplish it without this solid supposition.

Access Control: Unapproved and denied clients can't get to the cloud asset at whatever pointt.Once the client is denied, the gathering administrator makes the new encryption key for the particular gathering and transmits in a scrambled arrangement. Second the gathering trough refreshes the entire information list in the cloud server. Third the gathering oversees refreshes the client list and initiates the key for get to.

Efficiency: Get-together people inside the get-together can store and offer data records to others in the gathering by the cloud.

Secure Deduplicatoin: Secure deduplication requires that the cloud server can limit the storage room by keeping just a single duplicate of substance a similar document. Deduplication is a procedure to enhance information quality by expelling excess or redundant data from information away to enhance stockpiling use.

IV. SAAA MODEL - IMPLEMENTATION

A.Advantages of the SAAA Model

- The users can securely obtain their private keys from group manager.
- User send request to group manager for access the wanted group, at that time our system provide individual secure key to user without activation.
- Then group manager see the requests and activate the keys after confirm them.
- After user's private key gets activation, then only user can access the group.
- Our plan have fine-grained get to control, any client in the gathering can utilize the source in the cloud and disavowed clients can't get to the cloud again after they are repudiated.
- In our proposed framework the gathering chief plays out the beneath undertakings when a new customer joins the social affair or a customer has left the particular get-together,*Update the whole user name list.*

- *Generate a secure key and encrypt the key without activation and send to the updated user list.*
- *Update the rights in the cloud server.*

- We proposed public cloud named CloudMe for data storage.
- Group manager makes sure that the disavowed clients can't get to the record on the off chance that they contrive with untrusted cloud.
- In this work, we demonstrate a safe framework outline along this heading, which intends to unite the progressions of video coding procedures and secure deduplication of content record, picture and recordings getting transferred in the cloud condition to enhance the storage room.
- Media files like image and videos were eliminated in the recent surveys, we proposed to develop a unique architecture to prevent collusion attack and avoid replica of text, image and videos.

B. Operations of the Proposed System

Now we describe the operations of our proposed system.

Privacy preserving:

In this paper we address the issue of security saving information mining. In particular, we consider a condition in which two social events owning private databases wish to run an information mining calculation on the relationship of their databases, without uncovering any trivial data.The protection safeguarding information mining procedures are grouped in light of bending, affiliation lead, shroud affiliation govern, scientific classification, bunching, acquainted characterization, outsourced information mining, circulated, and k-secrecy, where their striking focal points and drawbacks are accentuated.

KNN:

In design acknowledgment, the k-closest neighbor's calculation (KNN) is a non-parametric method used for request and backslide. In the two cases, the data involves the k closest planning cases in the segment space. KNN is a sort of illustration based learning, or emotionless acknowledging where the limit is simply approximated locally and all figuring is yielded until course of action. The KNN estimation is among the minimum troublesome of all machine learning computations.

Deduplication:

Deduplication is a procedure to enhance information quality by expelling excess or redundant data from information away to enhance stockpiling usage, improve ETL, and upgrade information exchanges. Associations regularly don't have perceivability into the sources or reasons for repetitive information. Along these lines they have no chance to get of knowing how much excess information is costing them. For instance, a retailer can squander a considerable measure of cash sending various duplicates of a similar inventory or battle to one imminent client. By deduplicating the information early the organization can forestall squander.

SVC:

Adaptable Video Coding (SVC) is the name for the Annex G augmentation of the H.264/MPEG-4 AVC video weight standard. SVC arranges the encoding of an astonishing video bit stream that additionally contains no short of what one subset bit streams. A subset video bit stream is gotten by dropping packs from the more prominent video to lessen the data transmission required for the subset bit stream. The subset bit stream can address a lower spatial confirmation (more minor screen), chop down basic affirmation (chop down bundling rate), or lower quality video flag. H.264/MPEG-4 AVC was made generally by ITU-T and ISO/IEC JTC 1. These two social gatherings impacted the Joint Video To gathering (JVT) to build up the H.264/MPEG-4 AVC standard.

Collusion attack:

The customer leaving a particular social event are named as denied clients. The denied customers can not have the capacity to get the essential data annals once they are revoked paying little notice to whether they plot with the untrusted cloud. As needs be our proposed system perceives the repudiated customers and secures the data mystery and insurance.

Advanced Encryption Standard (AES):

The Advanced Encryption Standard (AES), for the most part called Rijndael (its phenomenal name), is a detail for the encryption of electronic information created by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael figure made by two Belgian cryptographers, JoanDaemen and VincentRijmen, who displayed a suggestion to NIST in the midst of the AES decision process. Rijndael is a gathering of figures with different key and square sizes.

AES chips away at a 4 × 4 section genuine demand system of bytes, named the state, but a couple of variations of Rijndael have a greater piece measure and have additional fragments in the state. Most AES estimations are done in a novel restricted field.

AES involves a couple of rounds of a couple of taking care of steps that join substitution, transposition and mixing of the information plaintext and transform it into the last yield of ciphertext.

Cloud Storage:

Clodu storgae is a model of information accumulating where the computerized information is secured in genuine pools, the physical putting away explores different servers (and often zones), and the physical condition is typically had and regulated by an empowering affiliation. These scattered amassing suppliers are in charge of keeping the information accessible and open, and the physical

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 1, Issue 11, DOI: 10.29027/IJIRASE.v1.i11.2018.209-215, May 2018

condition ensured and running. Individuals and affiliations purchase or rent amassing limit from the suppliers to store client, connection, or application information.

The get-together customer can move the archives in bona fide cloud server named cloudMe. Duplication of records are checked and the reports is been moved in the cloud server. To get a record, the client needs to send a demand to the cloud server. The cloud server will in like way check the client's character before issuing the relating record to the client. In midst of archive get to the customer key needs to facilitate by the social occasion executive and the requested record can be downloaded by the get-together customers.

V. PERFORMANCE ANALYSIS

A. Security performance comparison

When in doubt, our arrangement can achieve secure key allotment, get the chance to control, secure customer renouncement, unfriendly to scheme and data security are unmistakably watching the benefits of our proposed plot, as laid out in table 1, we list a table separated and Mona, which is Liu et al's. plot, the RBAC conspire, which is Zhou et al's game plan. The √ free means design can achieve the looking at objective.

TABLE 1. Security Performance Comparison

	Secure key Distribution	Access Conrol	Secure user Revocation	Anti-Collution	Data Security
MONA		√			
Secure RBAC on encrypted data		√			
SAAA Model	√	√	√	√	√

B. Deduplication Analysis

In general, our scheme can achieve secure deduplication with completely eliminate the extra storage, our scheme can achieve using scalable video coding techniques.This scheme is compared with table 2 and table 3, table 2(Before deduplication) contains no.of files, some file names and contents are repeated. So, storage space is occupied more. But in table 3(After deduplication) all file names are unique and contents are not repeated. So, storage space is consumed. We can achieve the corresponding goal.

TABLE 2. Before Deduplication

File Name	File size in bytes
dee.txt	3734
deepu.txt	3736
file.txt	3005
file1.txt	3291
graph.java	309
grapha.java	5398
file.txt	3005
deepu.txt	3734

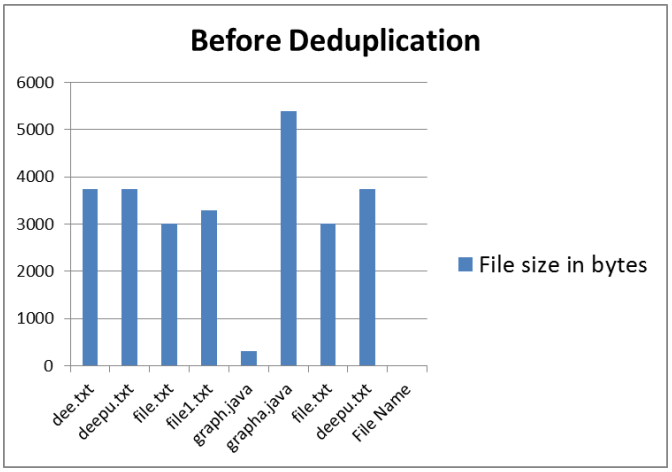

Fig 2. Before Deduplication

TABLE 3. After Deduplication

File Name	File size in bytes
dee.txt	3734
deepu.txt	3736
file.txt	3005
file1.txt	3291
graph.java	309
grapha.java	5398

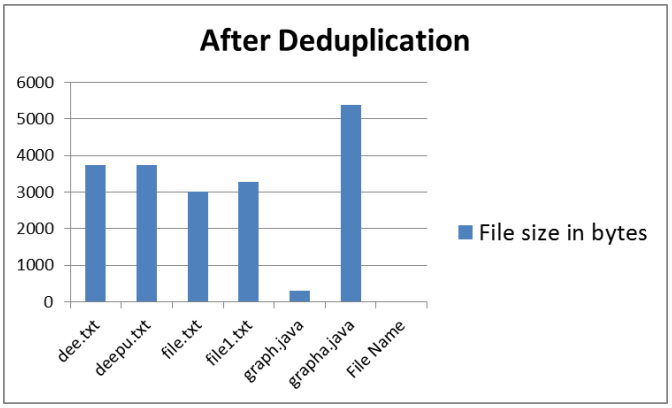

Fig 3. After Deduplication

CONCLUSION

Nowadays Cloud Computing is helping of sharing resources, services and data over the web among various users and industries. Thus, the security and privacy is the challenging issues in cloud computing. Our proposed plot gives a conceivable method to fight against shameless obstruction with the privilege of security. We trust more plans can be made to secure cloud client protection. Dynamic ownership administration is an imperative and troublesome issue in secure deduplication over scrambled learning in distributed storage. Security examination shows that our plans zone unit secure as far as corporate official and pariah assaults laid out in the arranged security display. furthermore

our arranged framework successfully defeats the plot assault. Additionally avoidance of putting away a same document like content record, picture and recordings will advance the client storage room and spares client storage room and cost.

In future, this exploration can be stretched out in two ways. Initial, a more nitty gritty plan of replication of documents will be directed including further advancement. Second, as replication of records definitely diminishes the replication level of Cloud information, the area of reproductions turns out to be more vital which merits additionally explore on enhancing information get to execution.

REFERENCES

[1] S. Ghemawat, H. Gobioff, and S. Leung, "The Google file system", in Proc, ACM symp.Oper. Syst. Principles, pp. 29-43, 2003

[2] E. Pinherio, W. Weber, and L. A. Barroso, "Failure trends in a large disk drive population", in Proc. USENIX Conf. File storage Technol., pp. 17-29, 2007

[3] Mohamed-K HUSSEIN, Mohamed-H MOUSA, "A Light-weight Data Replication for Cloud Data Centers Environment", International Journal of Engineering and Innovative Technology, Volume.1 Issue-6, June 2012

[4] Sumitra, "Comparative Analysis of AES and DES security Algorithms", International Journal of science and Research publications,Volume:3 Issue: 1, Jan-13

[5] Rohit Bajaj, "Developing Framework For Secure Storage In Cloud Computing System", International journal of New Innovations in Engineering and Technology,Volume-1 Issue 3, Feb-13

[6] Aarti.P Pimpalkar prof. H. A Hingoliwala," A secure cloud Storage System with Secure Data Forwarding", International journal of scientific & Engineering Research, Volume-4 Issue -6, Jun-13

[7] X.Liu, Y.Zhang, B. Wang and J. Yang, "Mona: Secure multi owner data sharing for dynamic groups in the cloud", IEEE Trans parallel distrib. Syst., Volume-24 Issue-6, Jun-13

[8] L. Zhou, V. Varadharajan and M. Hitchens, "Achieveing secure rolle-based access control on encrypted data in cloud storage", IEEE Trans. Inf. Forensics Security,volume-8 Issue-12, Dec. 2013

[9]J.yuan, S.Yu, " Secure and constant cost public cloud storage auditing with deduplication", IEEE conference on communications and Network Security, 2013

[10]Lukka Ramesh Babu, Vemu Tulasi, "High secure and verification mechanism for cloud storage", IJAIR, volume-2 Issue-7, 2013

[11] Rashmi, S. Ghavghave, Deepali, M. Khatwar, "Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm", International Journal on Recent and Innovation Trends in Computing and Communication,Volume:3 Issue: 5, May-15.

[12] Rohini Vidhate, V.D. Shinde, "Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI", International Journal of Multidisciplinary Research and Development, Volume: 2, Issue: 7, Jul-15

[13] Zhongma Zhu , Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", Ieee transactions on parallel and distributed systems, Volume-27 Issue -1, Jan-16

[14] Vishal R. pancholi Dr. Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES ",International journal for Innovative Research in Science & Technology, Volume:2, Issue:09, Februry 2016

[15] Wenhao Li, Yun Yang, Senior Member, IEEE, and Dong Yuan, Member, IEEE, "Ensuring Cloud Data Reliability with Minimum Replication by Proactive Replica Checking", Ieee transactions on computers, Volume- 65, Issue- 5, May-16.

[16] ASIA ABID, MOHAMMED KHALEEL AHMED, "Privacy Preserving Policy Based Content Sharing in Public Cloud", International journal of Advaced Technology and Innovative Research, Volume.08 Issue.15, October-2016,

[17] Junbeom Hur, Dongyoung Koo, Youngjoo Shin, and Kyungtae Kang, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage", IEEE Transactions on Knowledge and Data Engineering, 2016

[18] Yifeng Zheng, Xingliang Yuan, Xinyu Wang, Jinghua Jiang, Cong Wang, and Xiaolin Gui, "Towards Encrypted Cloud Media Center with Secure Deduplication", Ieee Transactions on Multimedia, 2016.

[19] K.Arul Jothy, K.Sivakumar, M J Delsey, "Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm", International Journal of Computer Science and Information Technologies, Volume 8 Issue-6, 2017