ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Efficient Data Integrity Checking with Group User Revocation in Cloud

Dhamale Swapnali[1], Bagul Sonali[2], Dhadge Madhuri[3], Garad Priyanka[4], Prof. Mrs.Sonali A. Patil[5]

B.E. Student, Department of Computer, BSIOTR, Wagholi, Maharashtra, India[1,2,3,4]

Asst. Professor, Department of Computer, BSIOTR, Wagholi, Maharashtra, India[5]

ABSTRACT: Now a days some researchers believed on save data effectively and securely on cloud.On the other hand, these systems are stillnot secure beside the collusion of cloud storage server as well as revoked group users during user revocation inpractical cloud storage system. In previous paper we found that collusion attack an efficientpublic integrity auditing scheme with secure group user revocation based on vector commitment plus verifier-localrevocation group signature. We invented a concrete scheme. We propose a new structure called Decrypt key, whichprovides efficiency and reliability assurance for convergent key management on mutually user along with cloud storagesides. The design is to apply de-duplication to the convergent keys to influence secret sharing techniques. In particular,we build secret shares for the convergent keys and share out them across multiple independent key servers. Ourproposed system rigging the public checking and efficient user revocation, as well as also some fine assets, such asconfidently, efficiency, countability and traceability.There is efficient use of vector commitment and verifier local revocation groupsignature.

KEYWORDS: Public integrity auditing, dynamic data, vector commitment,group signature, cloud computing.

I. INTRODUCTION

The growth of cloud computing encourages the endeavours and organization to subcontract their data to third-party cloud service providers. This will progress the storage drawbacks of resource limit local devices. In recent times, various profitable cloud storage services, such as the simple storage service, data backup services, realistic cloud based Software Google Drive are built for cloud application. Ever since the cloud servers may return unacceptable results, it's because of server's hardware failure or software failure. Sometimes human maintenance may lead to problems. And malicious attack will lead to unacceptable loss or result of data. To prevent from this situation, we are in need of data integrity and accessibility. This data integrity and accessibility are helps to protect data of cloud users. It also helps to provide privacy to the user's data. The improvements and enhancements in cloud computing motivates organization as well as enterprises to outsource their data to third party cloud service providers (CSP's) which will result in improvements the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) on-line data backup services of Amazon and software like Google Drive,Dropbox,Mozzie,Bitcasa andMemopal built for cloud application. In some cases cloud server sometime returns invalid results such as hardware/software failure, malicious attack and human maintenance. Security and privacy of cloud user's data should be protected by data integrity and accessibility. To overcome the security issues of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme are not sufficient for practical application. For achieving the integrity and availability of remote cloud storage, some various solutions and their different variants have been proposed. In these solutions, when a scheme supports modification of data, it is known as dynamic scheme, otherwise static one. A scheme is publicly verifiable that means the integrity check of data can be performed not only by data owners, but also by the third party auditor (TPA). However, the focus of the dynamic scheme is on the cases where only and only data owner could modify the data of cloud. Recently, the development of cloud computing emerged some applications where the services of cloud can be used as a collaboration platform. In these software development environments, one or more than one (multiple) users in a group need to share source code as well as they needs to access, compile, modify and run the source code share by user at any time. The

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

new model of cooperation network in cloud provides the infeasibility of data for auditing the remote data, where only the data owner can update its data. It will result in terrific communication and computation to the data owner which causes the single point of data owner. To achieve multiple data operation, Wang et al. put forth data integrity based on ring signature. In the scheme, it does not consider the user revocation problem and the cost of auditing is linear to the data size and group size. To further raise up the previous scheme and support group user revocation, Wang et al. proposed a scheme based on proxy re-signatures. However, this scheme assumes that authenticated and private channels exist between the pair of entities and there is no collusion among them. Also, cost of auditing the scheme is linear to the size of the group. Another attempt to improve the previous scheme and make the scheme scalable, efficient and collusion resistant, Yuan and Yu designed a dynamic public integrity auditing scheme with group user revocation. However, in their scheme, the authors do not consider the secrecy of data among the group users. That means, their scheme could efficiently support plain text of data update and integrity auditing, while not cipher text data. In their scheme, if data owner shares group key among the users of group, revocation of any group user allow the group users to update their shared key. Also, the owner of the data does not take part in the user revocation phase, where the user revocation phase is itself conducted by the cloud. In this case, the malicious cloud server will result in collusion of revoked user and the cloud server where the cloud server could update data number of times as designed and provide a legal data finally. Cloud Storage service are such as simple storage services in online data backup services of amazon, and practical cloud based software Google drive, drop box, mozzie, bitcasa and memo pal have been built for cloud application. There is invalid result in cloud server such as server hardware, software failure, human maintenance and malicious attack. Rabin data dispersion scheme implemented for practical application and overcome above challenges.

II. RELATED WORK

In A large amount of researchers have committed significant concentration to the troubles on how to securely outsourcelocal pile up to remote cloud server. The problem of remote data integrity and availability auditing attacks theattestation of many researchers.

SagarikaDev Roy, et.al (2014) proposed a methodology for secure outsourcing oflinear Computations into the cloud environment. Outsourcing is a common procedure engaged in the business worldwhen the customer chooses to farm out a certain task to an agent for the benefit of the firm in terms of time and cost.They proposed methodology to detecting a malicious server, in an efficient result verification method.

YongjunRen, et.al (2012) proposed designated verifier provable data possession. This plays a major role in publicclouds. Designated verifier provable data possession is a matter of crucial importance when the client cannot performthe remote data possession checking. By using the system security model and homomorphism authenticator theydesigned a new scheme. The scheme removed luxurious bilinear computing process. Furthermore in this proposal, thecloud storage server is stateless and independent of the verifier. This is an important secure property of any otherschemes. In the course of security analysis and performance analysis, their scheme is secure and high efficiency.

BoyangWang ,et.al(2012)proposed the first privacy-preservingmechanism that allows public auditing on shared data stored inthe cloud.With cloud storage services, it is commonplace fordata to be not only stored in the cloud, but also shared acrossmultiple users. However, public auditing for such shared data, while preserving identity privacy remains to be an open challenge. By exploiting ring signatures to computethe verification information needed to audit the integrity ofshared data. With our mechanism, the identity of the signeron each block in shared data is kept private from a third partyauditor (TPA), who is still able to verify the integrity of shareddata without retrieving the entire file.

Jia Yu, et.al(2015) proposedCloud storage auditing which is viewed as an imperative service to corroborate the veracity of the data in public cloud. Existing auditing protocols are all based on the supposition that the Client's secret key for auditing is completely protected. Such assumption may not always be held, due to the probably weak sense of security and/or low security settings at the client. In most of the current auditing protocols would inevitably become

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

unable to work when a secret key for auditing is exposed. It is investigated on how to reduce the damage of the client's key revelation in cloud storage auditing, and provide the first handy elucidation for this new problem setting.The security proof and the performance analysis show that the projected protocol is protected and well-organized.

JingweiLi ,et.al (2015) proposed the cloud computing technology, this technology outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing .Aim is to achieve both data integrity and deduplication in cloud, they proposed two secure systems, namely SecCloud and SecCloud+. SecCloud introduces an auditing entity with a maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud.

Jiawei Yuan, et.al (2014) proposed a new method based on some modern procedures such as based on authenticationpolynomial tags and linear authenticators. Data integrity auditing is achieved concurrently in this approach. Theproposed idea is to characterize the constant real time communication and also the computational cost on the user's side. It supports both public auditing along with batch auditing process.Many data loss and corruption events are reported against the well-known cloud service providers, data owners, to resolve these issues they need to periodically audit the integrity of the ifoutsourced data. And also every cloud service providers must improve their efficiency of cloud storage. To minimizethe unnecessary redundant copies, the cloud storage servers would deduplication the data. By having only one or fewcopies for each file and making a link to the file for every user who asks the same file stored in the disk.

III. PROPOSED SYSTEM

In this paper, we study the problem of constructing public authentication inspection for shared dynamic data with group user revocation. Our contributions are:

1) For cipher text database, we explore on the secure and efficient shared data integrate auditing for multi-useroperation.

2) We intend an efficient data auditing scheme along with new features such as traceability and countability by incorporating the vector commitment primitives, asymmetric group key agreement and group signature.

3) The analysis results show that our scheme is secure and efficient as we provide the security and efficiency analysis of our scheme which will result in back-up and data storage in cloud.

4) The authorized duplicate check in the hybrid cloud architecture is supported by several de-duplication constructions and this authorized duplicate check scheme comparatively incurs minimum overhead than normal operations.

The conventional encryptions have need of particular users to encrypt their data, with the own keys of the user.Therefore, the same data copies of different users will lead to dissimilar cipher texts. It creates integrity checkingprocess is an impossible task. Data outsourcing hoist security and privacy worry. We need to trust third-party providersfor proper implementation of confidentiality, integrity checking, and access control mechanisms. The present systemuse standard encryption scheme for identifying duplicate blocks, the blocks are stored in cloud. In Cloud Storage,standard encryption of identical files generates same key and same cipher text. As a result Data de duplication isimpossible in encrypted data. When user lost the key, there was impossible to restore the original content of the file.Message digest algorithm provides a viable option to enforce data confidentiality while realizing duplication.

It encrypts or decrypts a data copy with the help of a convergent key. By computing cryptographic hash value of thecontent of the data copy we can obtain the key. After key generation process and data encryption process, users canhang on to the keys. Then the user sends the cipher text to the cloud environment. Ever since encryption isdeterministic, the same data copies will generate similar convergent key and the identical cipher text. This permits the cloud to perform de-duplication over the cipher texts. Cipher texts are able to decrypt by the corresponding user's

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

withtheir convergent keys. Convergent encryption practical is to efficiently and reliably manage a huge number ofconvergent keys.

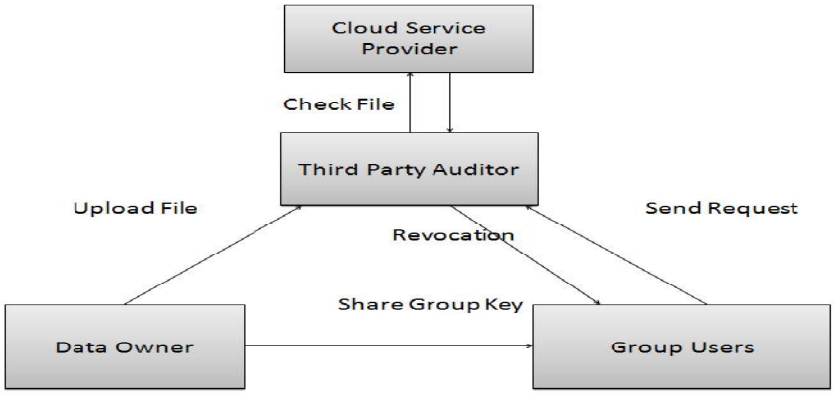

Fig1. System Architecture.

The unique Data block will be selected and those blocks are placed in the cloud service provider's space. We are using crypto graphic algorithm for integrity checking. Message authentication code is the scheme of producing Message digest for input file. The integrity checking should be done by Third party auditor by checking this message digest code.Before uploading file; data owner must send the hash key to the third party auditor. Third Party Auditor receives the key and verify with cloud service provider to check whether this file is already uploaded or not. In this module, user revokes the content by getting secret key of data owner. Data owner must share the secret key for group users. User downloads the file from the cloud service provider using hash key.

IV. REQUIREMENT ANALYSIS

HARDWARE RESOURCES REQUIRED

1. CPU Speed 1 GHz Remark Required
2. RAM 2 GB Remark Required
3. Hard Disk 320 GB Required
4. Mouse 3 Buttons Required

SOFTWARE RESOURCES REQUIRED

1. Operating System: window XP or Windows 7
2. IDE: Netbeans 7.3.1
3. Programming Language : Java
4. Back End: Mysql 5.5
5. Java: JDK 1.7

V. PROPOSED ALGORITHM

1. **AES Algorithm:**
2. Derive the set of round keys from the cipher key.
3. Initialize the state array with the block data (plaintext).
4. Add the initial round key to the starting state array.
5. Perform nine rounds of state manipulation.
6. Perform the tenth and final round of state manipulation.
7. Copy the final state array out as the encrypted data (ciphertext).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

2. Data Partition Algorithm- To divide data into fragments

Algorithm for fragments replication

For each Ok in O do

Select Si that has max(Rik +Wik)

ifcolSi = open color and si>= ok then

SißOk

Si ßsi – ok

colSißclosecolor

Sißdistance(Si; T) P /*returns all nodes at distance T from Si and stores in temporary set Si'*/

colSiß close color

end if

end for

VII.MATHEMATICAL MODEL

Let S be the whole System,
S = (I,P,O) where,
I-input, P-procedure, O- Output
I = (I0,I1,I2,I3,I4,I5)
I0= user id
I1= File to upload on cloud
I2 = No of Group Members
I3= Clouds Details
I4= User Activity
I5= Vector Commitment
P= (P0,P1,P2,P3,P4)
P0= Login to the cloud
P1= Create Cloud account
P2= Upload File to cloud
P3=Share File to group
P3= Monitor User Activities
P4=File integrity Checking.
P5= Revoke group user
P6= Invoke group user
O= (O1,O2)
O1= Data Integrity
O2=Revoked Group User

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

VIII. EXPERIMENTAL RESULTS

Fig2. User Registration

To register user needs enter email, password, name, mobile number, select group and address. All details are valid. Details are wrong registration is fail.

Fig3. User Login

User login time user enter email and password, system send security code you enter email.

Fig4. User Home Page

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

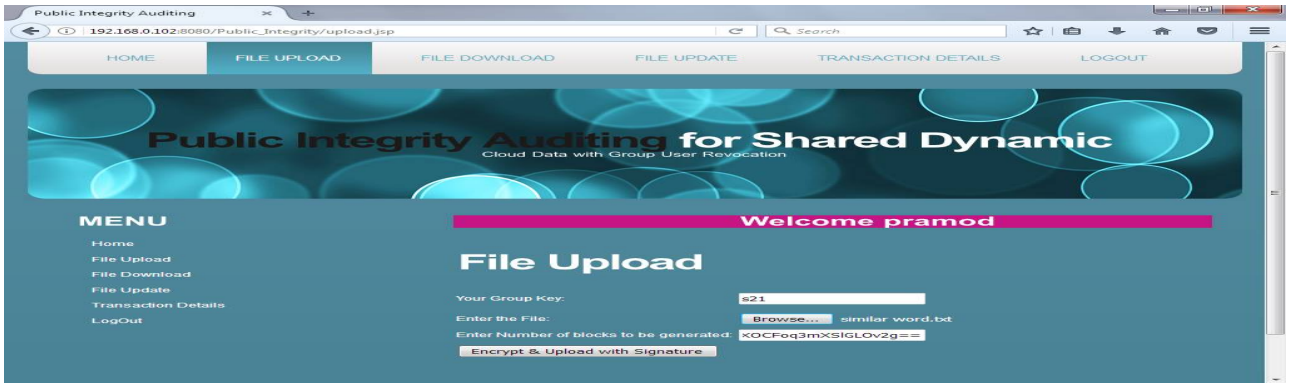

Fig5. File upload

You can select text file other file cannot accept here.

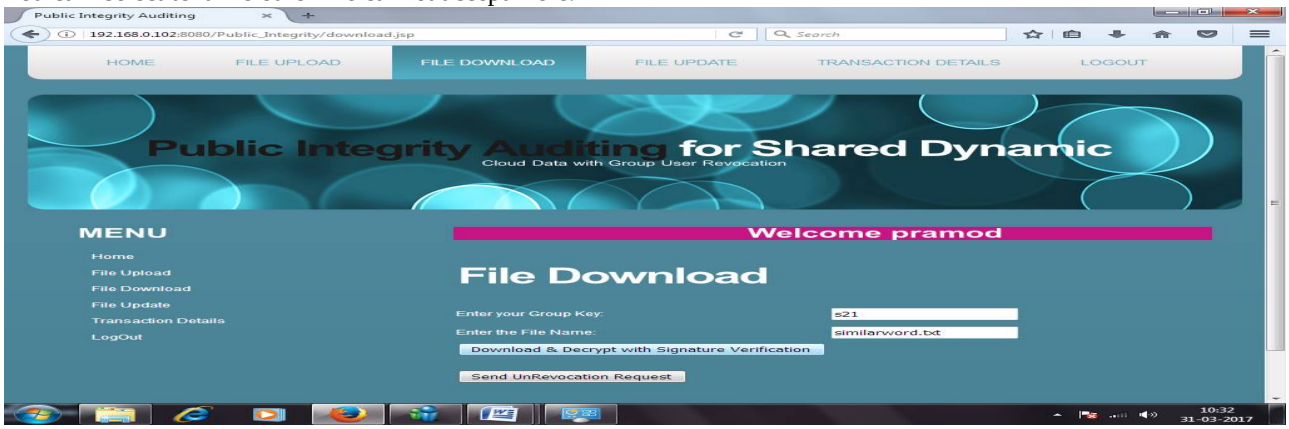

Fig6. File Download

You can enter group key, your require file name enter and download file.

Fig7. File Update

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

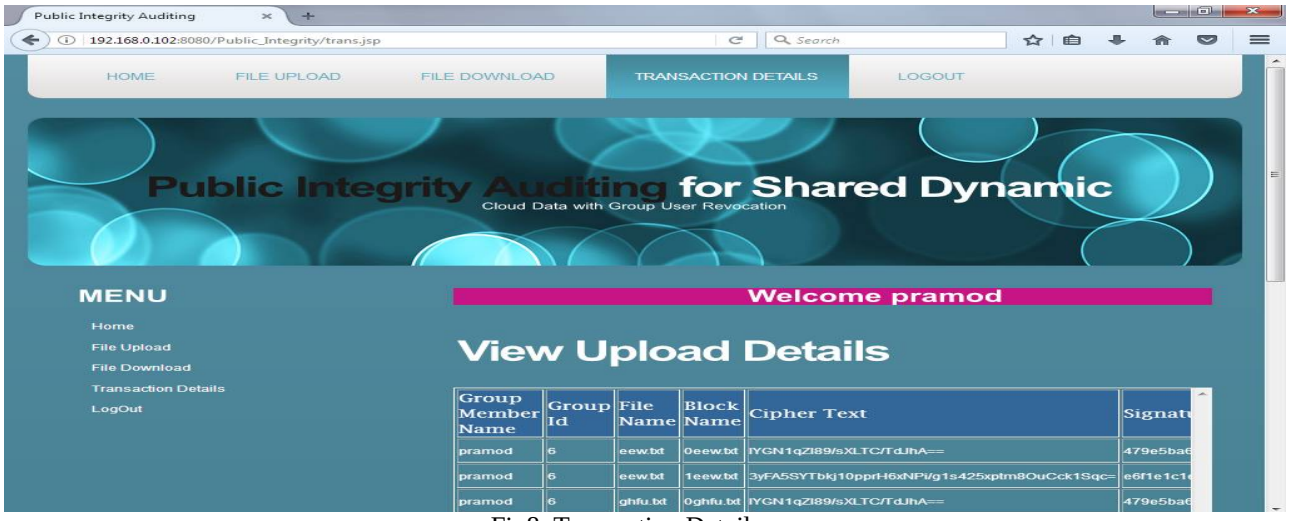

Fig8. Transaction Details

The following analysis graph shows that to encrypt and partition of our file data not vary to much with file. To complete this analysis we perform execution on different files of different size. In this first size is of very small size till it taking same time as the file of size 1500 byte is taking. This time taken is for the operations such as key generation, file encryption, file partition and file upload on cloud.

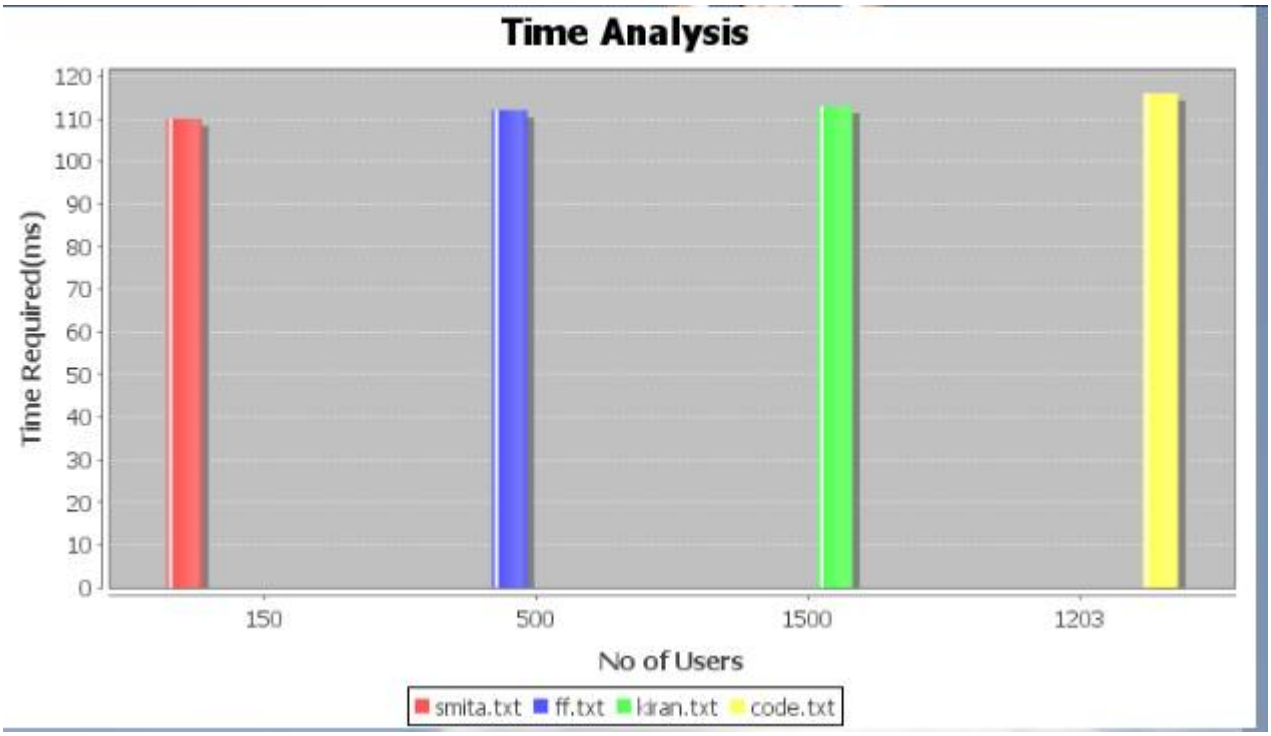

Fig. 9 Time Analysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IX. CONCLUSION

The data fileis securely sharedamong thedynamic groups. Membercan sign the same group and share the data efficiently without revealing user's identity.Cryptographytechnique is used for over all security.When AES and DES algorithms are compared, the key size of DES algorithm is very small so itspossible to hack easily.AES algorithm is used for efficient user revocationwithout updating private keys of remaining users. The proposed system is to realize efficient and secure data integrity auditing for dynamic data. The proposedmodel consists of the public data auditing and group user revocation. AES and Data partition algorithm techniquesprovides better data confidentiality.

REFERENCES

1. Dhamale Swapnali, Bagul Sonali, Dhadge Madhuri, Garad Priyanka, B.E. Student, Prof. Sonali A. Patil, Asst. Professor," A Survey on Efficient Data Integrity Checking with Group User Revocation in Cloud"in Dept. of Computer Engineering, BSIOTR, Wagholi, Maharashtra, India
2. Ashlesha Khatke,Neha Sharma,Sachin Kade,Sayyad Sofia, BE. Student, Prof. Sonali A. Patil, Asst. Professor," Security Analysis Using Probabilistic OPE Based Cloud Searching"in Dept.of Computer Engineering, BSIOTR,Wagholi, Maharashtra, India.
3. T. Jiang, X. Chen, an J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015
4. Jin Li, Yan Kit Li, X. Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorize Deduplication," in Proc. of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM VOL:PP NO:99 YEAR 2014.
5. Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" in Proc. Of IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 201X.
6. C. Wang Student Member, IEEE, Sherman S.-M. Chow, Q. Wang, Student Member, IEEE, K. Ren, Member, IEEE, and W. Lou, Member, IEEE , "Privacy-Preserving Public Auditing for Secure Cloud Storage".
7. B. Wang, B. Li, Member, IEEE, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" in Proc. Of IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 201X
8. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp. 525– 533.
9. D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.
10. B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912IJCATM:www.ijcaonline.org.