International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-09, Dec 2017

Reducing The Data Attacks on The Cloud by Dividing & Replicating The Data Over Multiple Cloud Nodes with Memory Managment

[1]Prof. Khan Faisal Ali, [2]Kanade Kalpana

[1]Asst Professor, [2]P.G. Student, Department of Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, Maharashtra, India

Abstract - In cloud computing, security and privacy are very important issues. In one hand, the user should authenticate itself before initiating any transaction, and on other hand user privacy also required so that the cloud or other users do not know the identity of the user. In this scheme introduce a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the users identity before storing data by using ABS (Attribute-Based Signature). The proposed scheme also has the added feature of access control in which only valid users are able to decrypt the stored information by using ABE (Attribute-Based Encryption).The proposed scheme support the de-duplication checking of files at cloud server. The scheme prevents replay attacks and supports creation, modification and reading data stored in the cloud. The proposed authentication and access control scheme is decentralized and robust.

Keywords: Cloud Security, Cloud Computing, fragmentation, Replication, Deduplication and Decentralized Access Control in cloud.

I. INTRODUCTION

Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technologies implementation (virtual machine (VM). The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. [1]

The main aim of our project is secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security. This system select the nodes in a manner that they are not adjacent and are at certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.[2][3]

Develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed System scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. This system do not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. this system en- sure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.[4]

In this paper, this system collectively approaches the issue of security and performance as a secure data replication problem. This system present Division and Replication of Data in the Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (this system use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. [5]A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, this system select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring.

Then other hand Cloud computing is a new computation model in which computing resources is regarded as service to provide computing operations. This kind of computing paradigm enables us to obtain and release computing resources rapidly. So this system can access resource- rich, various, and convenient computing resources on demand. [7][8].

The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers. Many applications use complex access control mechanisms to protect encrypted sensitive information. Sahai and Waters addressed this problem by introducing the concept for ABE. This kind of

new public-key cryptographic primitive enables us to implement access control over encrypted files by utilizing access policies associated with cipher texts or private keys. Two types of ABE schemes, namely key-policy ABE (KPABE) and cipher text- policy ABE (CP-ABE) are proposed. For KP-ABE scheme, each cipher text is related to a set of attributes, and each users private key is associated with an access policy for attributes. [9][10]

A user is able to decrypt a ciphertext if and only if the attribute set related to the cipher text satisfies the ac- cess policy associated with the user s private key. For CP-ABE scheme, the roles of an attribute set and an access policy are reversed. Bettencourt provided a CP-ABE scheme, which ensures encrypted data is kept confidential even if the storage server is untrusted. In order to withstand collusion attack and avoid sensitive information leakage from access structure, Qian et al. proposed a privacy-preserving decentralized ABE scheme with fully hidden access structure. Deng et al. constructed a cipher text-policy hierarchical attribute based encryption (CP-HABE) with short cipher texts, which enables a CP-HABE system to host many users from different organi- zations by delegating keys. In CPABE scheme, a malicious user maybe shares his attributes with other users, which might leak his decryption privilege as a decryption black box due to financial profits[11].

An area wherever access management is wide being employed is health care. Clouds area unit being employed to store sensitive information concerning patients to alter access to medical professionals,hospital employees, researchers, and policy manufacturers. It is vital to regulate the access of information so solely authorized users will access the information. Using ABE, the Records area unit encrypted beneath some access policy and keep in the cloud. User's area unit given sets of attributes and corresponding keys. Only if the users have matching set of attributes, will they rewrite the data keep in the cloud. Access management in health care has been studied in [12] and [13].

Access management is additionally gaining importance in on-line social networking wherever users (members) store their personal information, pictures, and videos and share them with elect groups of users or communities they belong to. Access control in on-line social networking has been studied in [19]. Such knowledge square measure being hold on in clouds. It's important that solely the licensed users square measure given access to that information. An analogous state of affairs arises once knowledge is hold on in clouds, as an example, in Drop box, and shared with sure groups of individuals.[14]

In computing, data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data. Related and somewhat synonymous terms are intelligent (data) compression and single-instance (data) storage. This technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. In the deduplication process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis. As the analysis continues, other chunks are compared to the stored copy and whenever a match occurs, the redundant chunk is replaced with a small reference that points to the stored chunk. Given that the same byte pattern may occur dozens, hundreds, or even thousands of times (the match frequency is dependent on the chunk size),the amount of data that must be stored or transferred can be greatly reduced

II. RELATED WORK

Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. Moreover, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies. User module uploads the text file on the cloud storage. Then the admin module fragments the file using algorithms and store on each node. Presented a technique to ensure the integrity, freshness and availability of data in a cloud. The data migration to the cloud is performed by the Iris file system. A gateway application is designed and employed in the organization that ensures the integrity and freshness of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. The proposed technique in heavily depends on the users employed scheme for data confidentiality. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on the traditional cryptographic techniques for data security.[15][16]

In ABE Attribute based encryption, this system considers the case that the user Alice has a large number of data stored in the cloud. If Alice submits a request for accessing the encrypted data stored in the CSP, according to the traditional outsourced ABE scheme, the CSP downloads all the data, executes partial decryption and responses all corresponding data of Alice. This greatly increases the cost for communication and storage at Alice side. In this article, this system organically integrates outsourced -ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE). In our system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the ciphertext only if their access policies satisfy the corresponding attributes. By this way, when Alice submits the request with a trapdoor corresponding to a keyword "current", CSP downloads all the data intended for Alice and just returns a partial ciphertext associated with the keyword "current". Therefore, Alice can exclude the data what she does not hope to read.[17]

III. OBJECTIVES OF PROPOSED SYSTEM

- To Avoid De duplications of Files over the cloud.
- Making replicas of files by using T-coloring Method by this any introducer not able to locate the files where actual data is located.
- If any introducer will get file over the nodes that time also he cant able to view the data in file because that single files are get fragmented on different nodes into the cloud.
- By Avoiding de-duplications of files users can get more space for utilization of cloud data because repetitions' of files cannot be accepted.
- Integrity checking of blocks at cloud server with the help of Third Party Auditor.
- Only authenticate user can access data because of unique key provided by service provider.
- The identity of the user is protected from the cloud during authentication
- Provide security to the data by encryption technique.
- Rights of files given by service provider only by this user van able to download modified and update his data.

IV. PROPOSED METHODOLOGY

1. User module

Data Owner (DO): This is a participant who intends to upload and share his data files on the cloud storage system in a secure way. The encrypted cipher texts will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in cipher texts, that is to say the predicate. The responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

Data User (DU): This is a participant who decrypts the encrypted data stored in S-CSP with the help of D-CSP. If the attribute set for DU satisfies the access structures, DU is able to access the encrypted files and recover the original files from it. DU downloads intended cipher texts with the help of trapdoor associated with appointed keyword. Data user is responsible for choosing keywords to create trapdoor, and decrypting data.

Key Generation Cloud Service Provider:

Trusted Authority (TA): TA is the attribute authority center, which is responsible for the initialization of system parameters, and the generation of attribute private keys and trap- door.

Key Generation Cloud Service Provider (KG-CSP):It a participant that supplies out- sourcing computing service for TA by completing the costly key generation tasks allocated by TA.

Decryption Cloud Service Provider :

Decryption-Cloud Service Provider (D-CSP):It is a participant that supplies outsourcing computing service through accomplishing partial decryption for cipher texts and key- word search service on the partially decrypted cipher texts for data users who want to access the cipher text.

Storage-Cloud Service Provider (S-CSP): It is a participant that supplies out sourcing data storage service for users who want to share file in cloud.

2. Data Division(Fragmentation)/Replication Module:

The file fragmented means to be broken up into small pieces. This is exactly what happens to files when they become fragmented. They are broken down into small individual pieces and stored in random locations. This causes less than optimal processing times because it takes longer to read through and find all of the different locations of the file, instead of being able to look in just one location. In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n multiples nodes, one fragment per node. The user can reconstruct file f by accessing m fragments arbitrarily chosen.

3.1 Data Fragmentation

The security of a large-scale system, such as cloud depends on the security of the system as a whole and the security of individual nodes. A successful intrusion into a single node may have severe consequences, not only for data and applications on the victim node, but also for the other nodes. The data on the victim node may be revealed fully because of the presence of the whole file [17]. A successful intrusion may be a result of some software or administrative vulnerability [17]. In case of homogenous systems, the same flaw can be utilized to target other nodes within the system. The success of an attack on the subsequent nodes will require less effort as compared to the effort on the first node. Comparatively, more effort is required for heterogeneous systems. However, compromising a single file will require the effort to penetrate only a single node. The amount of compromised data can be reduced by making fragments of a data file and storing them on separate nodes [17, 21]. A successful intrusion on a single or few nodes will only provide access to a portion of data that might not be of any significance. Moreover, if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low.

3.2 T-coloring

Suppose we have a graph G = (V;E) and a set Tcontaining non-negative integers including 0. The Tcoloring is a mapping function f from the vertices of V to the set of non-negative integers, such that Sf(x)- f(y)S ¶ T, where (x; y) > E. The mapping function f assigns a color to a vertex. In simple words, the distance between the colors of the adjacent vertices must not belong toT. Formulated by Hale [6], the T-coloring problem for channel assignment assigns channels to the nodes, such that the channels are separated by a distance to avoid interference.

3A. Proposed Model

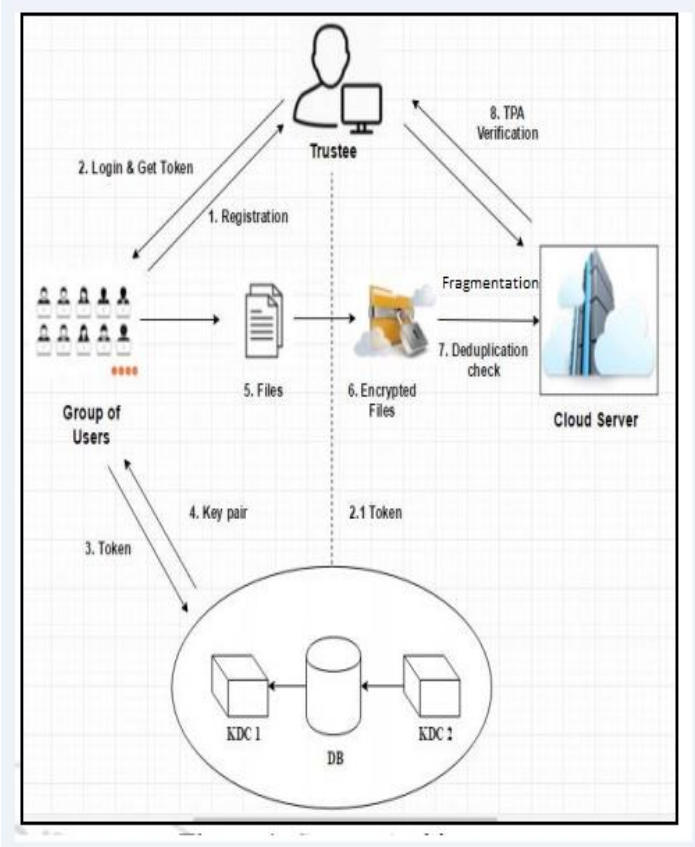

Figure 1: System Architecture

This is a privacy preserving authenticated access control scheme in which user can create a file and store it securely in the cloud using ABE and ABS protocol. The architecture is decentralized, meaning that there are several KDCs for key management. There are three different users, a creator, a reader and writer. Creator receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. For example, these can be servers in different parts of the world. A creator after validating the token to one or more KDCs, receives keys for encryption/decryption and signing. The message is encrypted under the access policy. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy, to prove his/her authenticity and signs the message using this claim. The cipher-text with signature is sent to the cloud. The cloud verifies the signature and stores the cipher-text. [18]

Writing process is similar as file creation. By assigning the verification process to the cloud, individual users are relived from time consuming verifications. When a reader wants to read data in the cloud, it tries to decrypt data in Cipher-text form using the secret keys it receives from the KDCs. If user has sufficient attributes matching with the access policy, then he/she can decrypt the information stored in the cloud.

The main modules are

1. Trustee

A trustee can be someone like the federal government who is responsible for managing social insurance numbers etc.

2. KDC

The function of KDC is to distributes secrete key and writer key to all authentic users. Cloud has many KDCs in different locations in the world.

3. Creator

Authorized Creator can write the file and upload to the cloud.

4. Client

(a) Reader

Reader can read the file online with help of secret key (SK)

(b) Writer

When the writer want to upload or modify file then if the writer key valid

then he/she can update the article.

5. Cloud Server

Cloud server is used to storage of data where user can upload the data. When user wants to upload files first he/she has to send request to KDCS

3B. Experimental Analysis

Figure1: MultiCloud System Environment

Administrator can having the Access to handle the cloud System

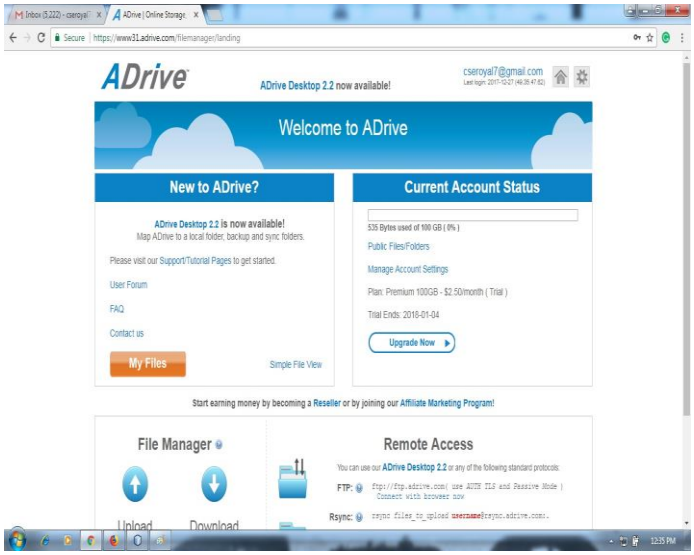

Figure2: ADrive is the Google Drive can used to access the cloud with a proper Administrative control.

Figure3: Administrator have only access to authenticate the Users only.

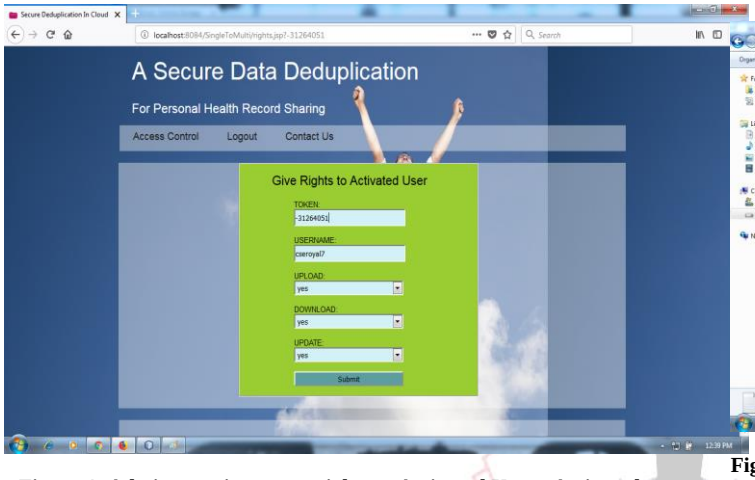

Figure 4: Admin can give access rights to Activated Users. Activated User can access the all the data files within the cloud.

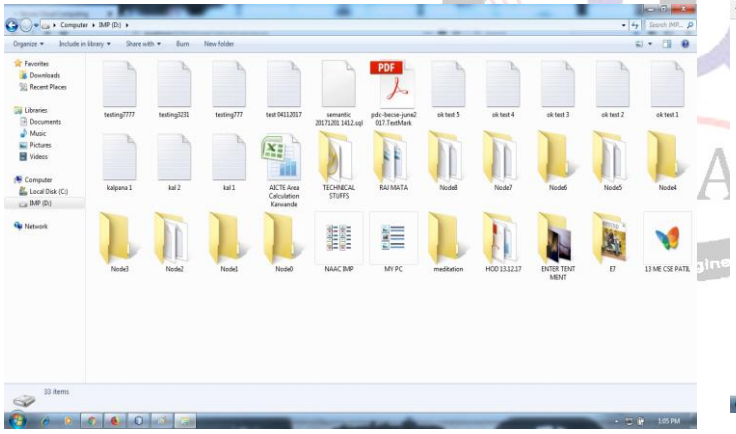

Figure 5: User can create the no of node for fragmented file.

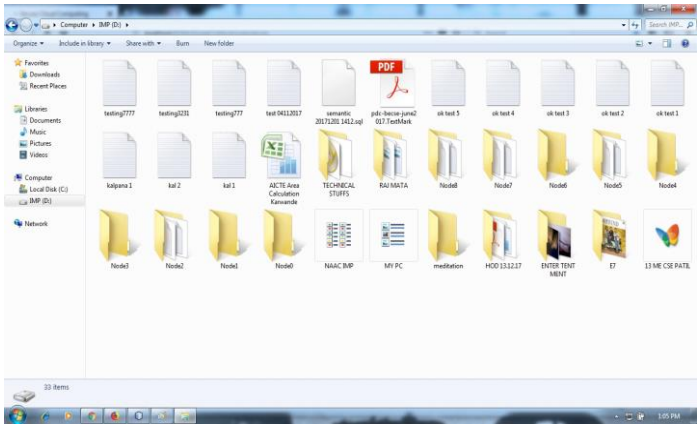

Figure 6: User can view the saved file or access the file update or rename the file to avoid deduplication.

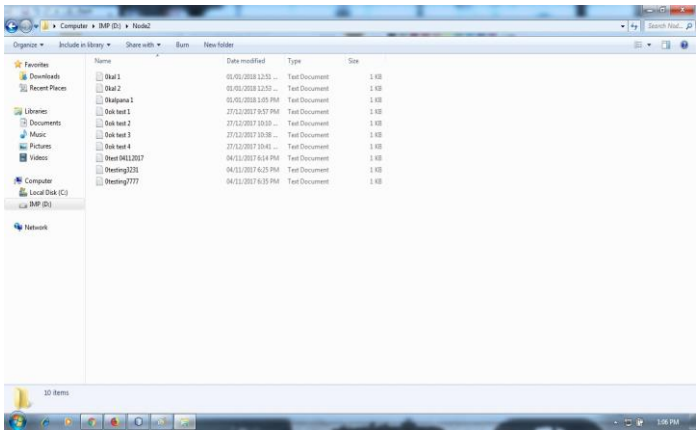

Figure 7: No of data files are viewed in specified node in a cloud

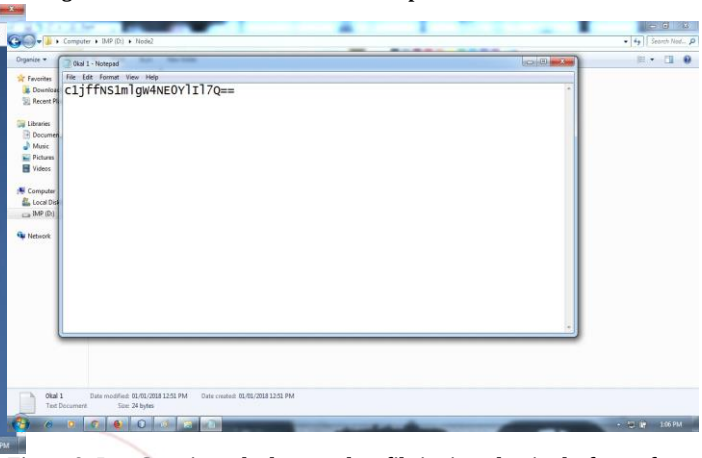

Figure 8: In a Certain node the save data file is viewed as in the form of encrypted file, which is not understandable to other users.

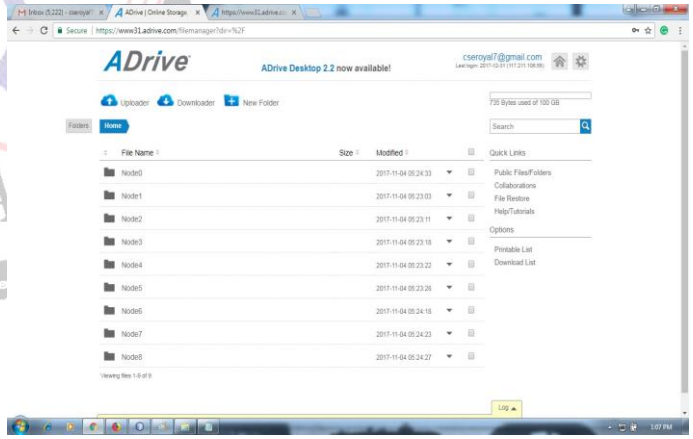

Figure 9: The Cloud ADrive contains the File Name such as Node0 to Node 8 which is modified with a certain date or particular size.

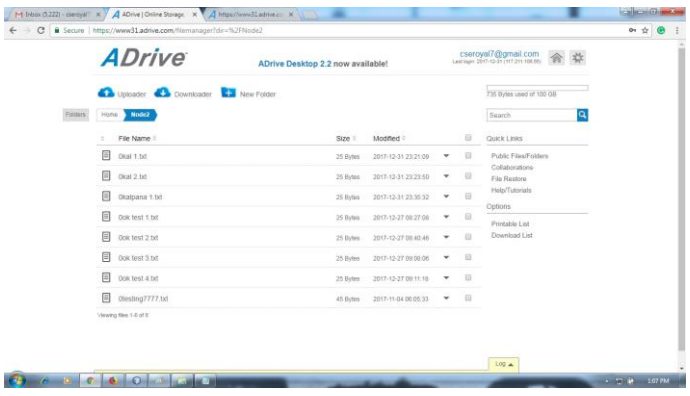

Figure 10: In a Cloud ADrive each individual nodes data files are uploaded, upadated with a active user.

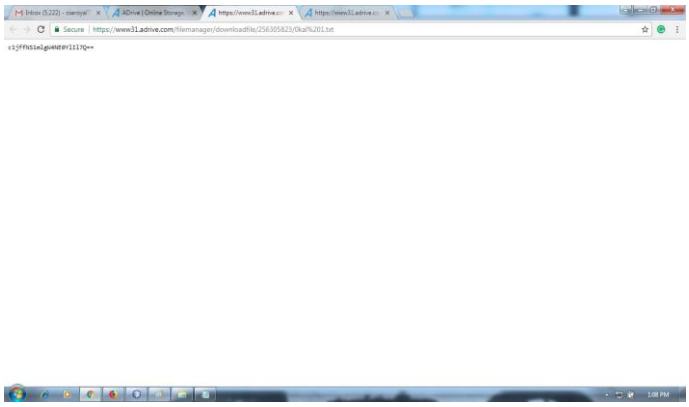

Figure 11: This is the Encrypted file not easily access by the user.

V. CONCLUSION

The decentralized access control technique with anonymous authentication, which provides de-duplication check and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. Also integrating checking is performed by Third Party Auditor on behalf of user request. As de duplication is performed before uploading the files at cloud server which reduces the storage overhead and also reduces the computation cost. One limitation is that the cloud knows the access policy for each record stored in the cloud.

REFERENCES

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Kaminski, Gunshot Lee, David Patterson, Ariel Rabin, Ion Stoical, and Matey Zaharias,ˆa Above the Clouds: A View of Cloud Computing

[2] Chui Ran, Cong Wang, and Ian Wang, "Security Challenges for the Public Cloud"

[3] Giuseppe Agenise, Randal Bursa Reza Carmela, Joseph Herring, Lea Kisser, Zachary Peterson, Dawn Song, "Provable Data Possession at Entrusted Stores"

[4] C.Chris Elway, Alptekin Kupc AˆA¸ CharalamposPapamanthou, Roberto Tamassia, "Dynamic Provable Data Possession"

[5] Cong Wang, Member, Sherman S.M. Chow, Qian Wang, Kui Ren, WenjingLou,"Privacy-Preserving Public Auditing for Secure Cloud Storage"

[6] Boyang Wang, Baochun Li, Hui Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud"

[7] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to Leak a Secret"

[8] Anne Srijanya. K, N. Kasiviswanath, "Data Integrity Verification by Third Party Auditor in Remote Data Cloud"

[9] K.Kiran Kumar, 2K.Padmaja, 3P.Radha Krishna "Automatic Protocol Blocker for Privac Preserving Public Auditing in Cloud Computing"

[10] Jachak K.B., Korde S.K., Ghorpade P.P. And Gagare G.J., a Homomorphic authentication with random masking technique ensuring privacy security in cloud computing.

[11] C.Wang, Q.Wang, K. Ren,andW. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Intˆal Workshop Quality of Service (IWQoSa09), pp. 1-9, 2009.

[12] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[13] B.Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

[14] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22ndInt al Conf. Theory and Applications of Cryptographic Techniques: Advances In cryptography)pp. 416-432, 2003.

[15] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int al Conf. Theory and Application of Cryptology and Information Security:Advances in Cryptology (ASIACRYPT¨ Ea01), pp. 552-565, 2001.

[16] Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. 584-597.

[17] Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific Engineering Research, Volume 3,Issue 6, ISSN 2229-8 June 2012.

[18] D. Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science and Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011

[19] K Govinda, V. Gurunathprasad and H. satish kumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, vol4,no. 2,ISSN: 2249- 9954,4 August 2012

