Cloud Computing: Ensuring Data Storage Security in Cloud

Ms. Swati I. Bairagi[1], Dr. Pradip M. Jawandiya[2]

[1]M.E. Computer Science and Engineering Scholar, [2]Principal, P.L.I.T Buldhana
Pankaj Laddhad Institute of Technology and Management Studies,
Maharashtra, India
Sant Gadge Baba Amravati University, Amravati

***Abstract*- Cloud computing is a rising computing standard in which the computing framework is given as a service over the Internet. The Cloud computing tool gives facility of data storage and access for cloud users, but when outsourcing the data to a third party causes safety issue of cloud data so data are protected by restricting the data. We propose a new decentralized access control scheme for secure data storage in the clouds that supports anonymous authentication where identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. In addition to this a new symmetric key cryptographic method called Modern encryption Standard (MES)-II presents method which can be effective to encrypt various types of plain text files and the method is free from standard cryptography attacks namely brute force attack, known plain text attack and differential attack**

***Index Terms*- Cloud Storage, Decentralized Access, Key, Distribution Center, Anonymity Authentication, Key Management, SHA (Secure Hash Algorithm), MES-II.**

I. INTRODUCTION

Data stored at clouds are maintained by Cloud service providers (CSP) with various incentives for different levels of services. However it eliminates the responsibility of local machines to maintain data, there is a chance to lose data or it effects from external or internal attacks. To maintain the data integrity and data availability many people proposed several algorithms and methods that enable on demand data correctness and verification. So Cloud servers are not only used to store data like a ware house , it also provides frequent updates on data by the users with different operations like insert, delete , update and append. Lastly the deployment of cloud computing is powered by the data centers running in cooperated and distributed manner. Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works under different systems and security models. Researchers also proposed distributed protocols to ensure storage correctness across multiple servers we mainly focus on dynamic generation of tokens for verification of blocks and token pre computation before distributing the files in to cloud. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. For example, medical records and user-driven data generated in social networks are often stored in public or private clouds. Ensuring privacy and security of such data is important for users to trust the service providers. For achieving that, adequate authentication and access control techniques must be employed.

A high level security system also ensures that only verified and valid services are provided to authorize users. Indeed, the process of authentication must be initiated for all valid transactions that are performed through the cloud. The first goal of our work is to implement anonymous authentication of users. The privacy settings of users must be followed in such a manner that the identity of the user should not become evident to either the cloud service providers or to other users. Thus, the anonymity of users is preserved. To provide secure data storage, the cloud data needs to be encrypted. The second goal of our work is to ensure data privacy and security. Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. Numerous services like email, Net banking and so forth are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage

II. LITERATURE REVIEW

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters [12] introduced the concept of Attribute based encryption for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attributebased encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key.

John Bethencourt, Amit Sahai, Brent Waters[13]introduces Ciphertext-Policy Attribute-Based Encryption in 2008. The expert employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of our system and give performance measurements. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrate the basic principles on which an architecture for combining access control and cryptography can be built. then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power.

Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi[9]introduced Anonymity-preserving Public-Key Encryption:A Constructive Approach where public-key cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). Junbeom Hur, Dong Kun Noh[14] introduces the concept of Attribute-Based Access Control with Effcient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based cryptosystems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions.

The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a re-encryption that takes the ciphertext and reencrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devi[18] describes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. The scheme implemented secure cloud storage byproviding access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. Parjanya C.A and Mr. Prasanna Kumar M[16]describes the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in march 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

S Divya Bharathy and T Ramesh[15] intrdused the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized

SR. No	Year	Author	Advantages
1	2006	Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters	Introduces new cryptosystem for ABE encrypted data
2	2007	Matthew Pirretti and Brent Water	Information management architecture based on emerging attribute-based encryption (ABE) primitives and cryptographic optimizations in Secure Attribute Based Systems

3	2008	John Bethencourt, Amit Sahai, Brent Waters	introduces Ciphertext-Policy Attribute-Based Encryption and the confidentiality of the data will be compromised
4	2010	Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarat	Combine access control and cryptography. Allows policy changes and data updates at a limited cost in terms of bandwidth and computational power.
5	2012	Junbeom Hur, Dong Kun Noh	The attribute based crypto-systems were introduced such as Ciphertext Policy Attribute-Base Encryption (CP-ABE) with an addition of new functions.
6	2013	R.Ranjith and D.Kayathri Devi	Secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination
8	2014	S Divya Bharathy and T Ramesh	Supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds. , the cloud adopts an access control policy and attributes hiding strategy to enhance security
9	2014	Sushmita Ruj, Milos Stojmenovic, AmiyaNayak	The cloud verifies the authenticity of the series without knowing the user's identity before storing data. only valid users are able to decrypt the stored information.

Table 1: List of comparison of Existing System

Disadvantages of Existing system

- The identity of the user is not protected from the cloud during authentication.
- There can be only one KDC for key management.
- Access control of data stored in cloud is centralized.
- Two users can collude and access data or authenticate themselves, if they are individually not authorized. This is called collusion attack.
- Revoked users can also access data even after they have been revoked.
- Prone to replay attacks.
- Single read and writes on the data stored in the cloud.
- The scheme in uses asymmetric key approach and does not support authentication.
- Difficult to maintain because of the large number of users that are supported in a cloud environment.

III. PROPOSED SYSTEM

Objective

- Distributed access control of data stored in cloud so only authorized users with valid attributes can access them.
- Authentication of users who store and modify their data on the cloud.
- The identity of the user is protected from the cloud during authentication.
- The architecture is decentralized, meaning that there can be several KDCs for key management.
- Revoked users cannot access data after they have been revoked.
- The proposed scheme is resilient to replay attacks.
- The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

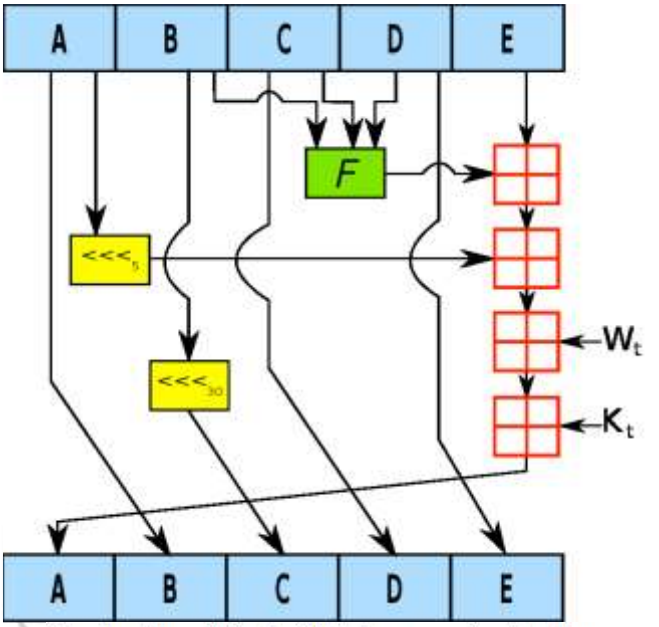
Following assumptions are made in the proposed system:

1. Users can have either read or write or both accesses to a file stored in the cloud.
2. All communications between users/clouds are secured by secure shell protocol, SSH.
3. The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing user's content, but cannot modify it

Algorithm Used

1. SHA-1(Secure Hash Algorithm)

It is used commonly with the Digital Signature Algorithm in electronic mail, electronic funds transfer, software distribution and various other applications that demand data integrity and authentication. The idea of signing hashed messages provides many advantages, one of them being faster creation and less resources for storage or transmission. SHA-1 is a hash function that takes a variable length input message and produces a fixed length output message called the hash or the message digest of the original message. The SHA-1 algorithm belongs to a set of cryptographic hash functions similar to the MD [Message Digest] family of hash functions. But the main difference between the SHA-1 and the MD [Message Digest] family is the more frequent use of input bits during the course of the hash function in the SHA-1 algorithm than in MD4 or MD5. This fact results in SHA-1 being more secured compared to MD4 or MD5 but at the expense of slower execution. The way this algorithm works is that for a message of size $< 2^{64}$ bits it computes a 160-bit condensed output called a message digest. The SHA-1 algorithm is designed so that it is practically infeasible to find two input messages that hash to the same output message. It is also practically impossible to deduce the original input message given only the output hash message.



One iteration within the SHA-1 compression function:
A, B, C, D and E are 32-bit words of the state;
F is a nonlinear function that varies;
$\lll_n$ denotes a left bit rotation by *n* places;
n varies for each operation;
W_t is the expanded message word of round t;
K_t is the round constant of round t;
$\boxplus$ denotes addition modulo 2^{32}.

Fig. SHA (Secure Hash Algorithm)

2. (MES)-II (Modern Encryption Standard)

A new symmetric key cryptographic method called Modern encryption Standard (MES)-II. One of the authors has published Modern Encryption Standard Version-I (MESI). In the present method there is a use of Modified generalized Vernam cipher method with feedback with different block size from left to right. The entire content of given data is divided in different block sizes. After that entire content is divided into two files and then combine them by taking 2nd half first and the 1st block. The generalized modified Vernam Cipher method again applied from left to right with different block sizes. The authors have proposed the present method and it can be effective to encrypt various types of plain text files and the method is free from standard cryptography attacks namely brute force attack, known plain text attack and differential attack. MES -II can be used as independent encryption algorithm to encrypt any short message such as SMS, Password or encryption key etc.

Encryption using MES-II

These are some important algorithms included for Encryption & Decryption along with various File operations algorithms, Key generation algorithms and Key manipulation algorithms namely- Encryption Algorithm: Main(), Decryption Algorithm:Main(), Function Vernam_Cipher: Feedback_Encryption(), FunctionVernam Cipher: Feedback_Decryption(), function keygen(), function randomizing key(), function filereverse(), function filesplitting(), function mergefile(), function filecopy(), function tictoc(), etc. The main module of Encryption takes names of the plain text file and cipher text file as input from the user. It also takes the key used for encryption as input and executes the complete encryption algorithm by calling the various functions involved in this encryption method. The methodology for encrypting the given data is explained in earlier section, which is meant for only Encryption purpose only. And at the receiver's end, the enciphered file is to be decrypted for getting the original plain text file. The Decryption process includes the general reverse process of Encryption method.

Algorithm for Encryption using MES-II

1 Start
2 Input file1(plaintext file)& open it in read mode
3 Input file2(cipertext file)& open it in write mode
4 Input File_key & open it in write mode
5 Generate random number
6 generate key using File_key & lenght of file1
7 randomize the key no. of times equal to file_len
8 call encryption function()
9 copy contents of encrypted file in some temporary file
10 call file_splitting() for splitting
temp file into sub files
11 call file_reverse() for reversing the content
12 call file_merge() for concatenation of filea to the end of fileb
13 again call encryption() for encrypting merged file
14 call file_copy() for copying the
encrypted contents from temp file to cipher text file2
15 close all files
16 delete temp files
17 stop

The present method is such that encrypted text cannot be decrypted without knowing the exact initial random key. To generate random key we can use a special random number generator function, we have used only generalized modified vernam cipher method with variable block size and variable key and also the encryption done in two ways. The proposed algorithm shows that the present method is free from standard cryptography attack such as known plain text attack, brute force attack, and differential attack.

IV. IMPLEMENTATION

- ***List of phases of work***

1. System Initialization
2. User Registration.
3. KDC setup.
4. Attribute generation.
5. Sign
6. Verify.

- **System Initialization:** The System Initialization is the initial process for the system. The system gets initialized for the user. The single user or the group of user can register within the system
- **User Registration:** The User has to register them under the registration module. According to the user credentials, which will be provided by the users, the user will get the private key. And by using that private key the user can then upload or download the required data in the future.
- **KDC setup:** We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.
- **Attribute generation:** the token verification algorithm verifies the signature contained using the signature verification. This key can be checked for the consistency. There are two types of access permissions are given to the user. Read and

read write access. The user will allow the user to only read the content of the sent file or they can permit to read and make some required modification and write it back again.

- **Sign:** The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.
- **Verify:** The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs.

- ***Technology basis***

Software Requirements

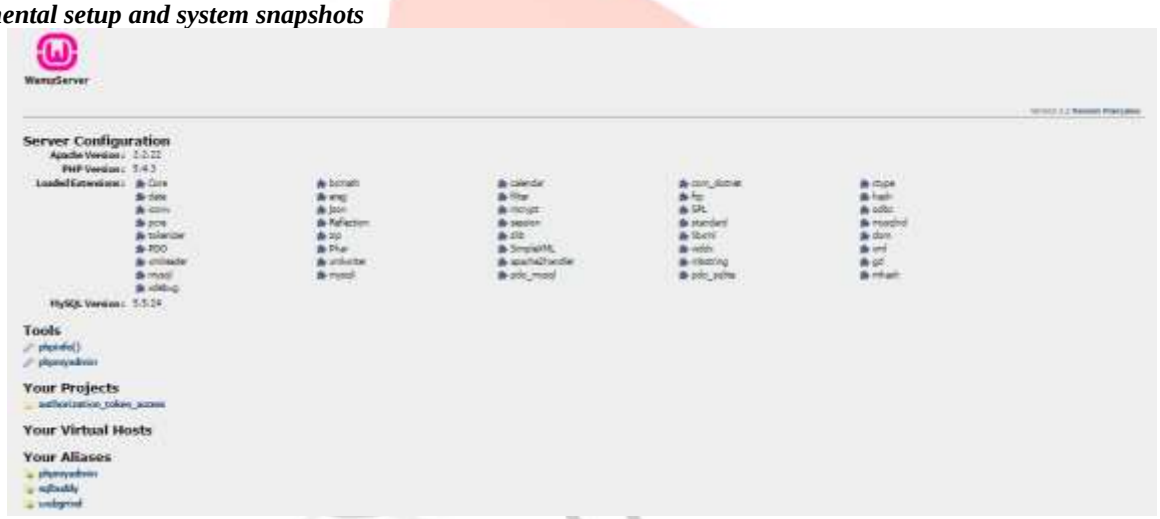
Front End: PHP
Back End: My Sql
Operating system: Windows XP, Windows 7
Browser: Mozilla Firefox, Internet Explorer, Google Chrome
Data Base: My Sql
Platform: WAMP Server 5.2

Hardware Requirement

System: Pentium IV 3.5 GHz.
Hard Disk: 40 GB

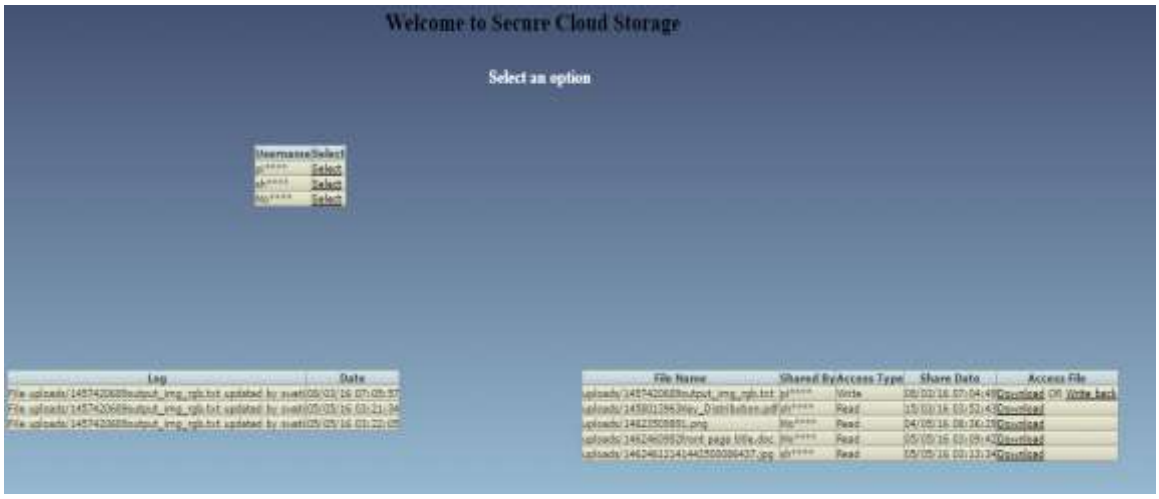
V. EXPERIMENTAL RESULTS AND DISCUSSIONS

Experimental setup and system snapshots



Screenshot1-Homepage of system

Screenshot 2: Login Page



Screenshot 3: KDC User Login

Screenshot 4: Select user and file to grant access

Screenshot 5: Upload New files Window

Result Analysis

1. **Analysis with respect to the distribution of the key**

In the single key distribution environment, the public key of all the users is maintained by the single KDC. The single KDC is responsible for all the encryption and decryption. Hence the load on the center is too much too handle such a large amount of key as the users of cloud are increasing day by day. Hence the burden of one KDC is divided into more than one KDC. The distributed environment has more than one KDC where the keys and the user attributes are distributed. As the one KDC is the single point of failure may breakdown the transaction hence the keys are distributed all over the KDCs.

2. **Analysis with respect to the privacy preserving Authentication**

The Authentication is to verify the user among the various users. Only Authorized user can access the data. The authentication process exceeds authorization. The authentication can be provided by obtaining the user id, username or password etc. According to the credentials that are received by the user can get verified uniquely. The authentication scheme is privacy preserving that it prevent the data to be access by any unauthorized user.

3. **Analysis with respect to the Access Policy**

The user can decide that which user can access his data, and which user can only read the data or can modify it and write back. There are 2 types of access policies, the only read policy permits user to only read the file and can only downloads the file. User can't make any changes through it. The read/write access permits the user to read the content of the file and if the user feels to change it then the file can be modify and user may write it back. This policy granting facility is depends upon the user itself. It depends completely on the user to grant the access permission to the user. The single write and single read permissions are granted by the many users. But the system proposes the many read and many write permission to the user.

4. **Analysis of time required for transaction on cloud**

File Size	Upload(Sec)	Download (Sec)
10bytes	15	0
1kb	17	3
10kb	19	0
100kb	20	7
1Mb	22	7

VI. CONCLUSION AND FUTURE SCOPE

In this paper we have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Privacy and the security are the two mentioned factor for the data stored on the cloud. User authentication ensures the security. Hence the data can be only visible to the user who is successfully authenticated to the system. The user may permit another user to access data by granting the access permission according to the choice. User Anonymity ensures the privacy of the data. The decentralized nature of the system relaxed it from the burden of maintaining the logs and attributes of the entire user. Key distribution is done in a decentralized way. In future will show what modification is done in the client file by server to the client. The user can view their file details such as upload files, download files. Modification files can view through accessing with the help of mobile.

VII. ACKNOWLEDGMENT

The real spirit of achieving a goal is through the way of excellence and lustrous discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities. I express thanks and gratitude to Head of Department, **Prof. V. P. Narkhede** for his encouraging support and co-operation in this seminar.

I would like to thank to my Project guide **Dr. P. M. Jawandhiya,** Principal, Pankaj Laddhad Institute of Technology and Management Studies, Buldana for their valuable support. He gave me the knowledge from his own experience. His guidance helped me in growing my confidence which would help me in my future. So I am sincerely thankful to my guide. At the same time, I would like to thank all teaching and non teaching Staff Members of my Department and my friends for their help.

REFERENCES

[1] Deepanchakaravarthi Purushothaman, Dr.Sunitha Abburu "An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012, ISSN (Online): 1694-0814.

[2] Nikita pathrabe, Deepali khtawar "Ensuring data storage security in cloud computing" International Journal of Research in Advent Technology, Vol.2, No.2, February 2014, E-ISSN: 2321-9637

[3] G.Divya1, K.Kuppusamy2" Data Storage Using Decentralized Access Control With Multiple Authentication in Clouds" IJCSMC, Vol. 4, Issue. 7, July 2015, pg.476 – 479, ISSN 2320–088X

[4] Swetha Maharajanavar," Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 4 2194 – 2197

[5] D. Kanchana, Dr. S. Dhandapani "A Novel Method for Storage Security in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[6] B.Anjani Kumar, K.Hari Prasad, C.Subash Chandra"Homomorphic Token and Distributed Erasure-Code for cloud",International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, October- 2013.

[7] B. Shwetha Bindu1, B. Yadaiah2**,"** Secure Data Storage In Cloud Computing" International Journal of Research in Computer Science ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 63-73

[8] Miss. Roopa G, Mr. Manjunath S "Secure Way of Storing Data in Cloud Using Third Party Auditor",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 69-74

[9] Surajkumar J. Manowar , A. M. Sahu" Introduction to Modern Encryption Standard (MES)-II: An independent and efficient Cryptographic approach for Data Security" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 310-313 ISSN-0975-9646

[10] SHA hash functions Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/SHA1#Description_of_the_algorithms

[11] URL:http://www.en.wikipedia.org/wiki/SHA-1

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[13] John. Bethencourt, A. Sahai, and B. Waters, "CiphertextPolicy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, May 2006

[14] A. Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Lui, "A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing, 2011

[15] S Divya Bharathy,T Ramesh,"Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control," Proc. IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1069 –1074.

[16] Mr. Parjanya C.A,Mr. Prasanna Kumar M," Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proc. IJARCSSE, Volume 4, Issue 3, March 2014

[17] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp., 2011.

[18] Ashwarya Joshi1, Amol There2, Akshay Kakde3, Suraj Dharaskar4, V. L. Kolhe5" Access Policy Control for Data Stored In Cloud" International Journal of Engineering Technology and Management (IJETM) Volume 2 Issue 2 Page No. 63-67, ISSN: 2394-6881