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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Data Security Scheme: Share and Audit Our Data into Cloud using Encryption

Ashvini Jangam, Prof. Nilesh Sable

Department of Computer Engineering, Imperial College of Engineering and Research, Wagholi, Pune, India

ABSTRACT: Cloud computing has been emerged as a computing network over the web. Cloud information indulge storing of the info within the cloud furthermore as has sharing capability among multiple users. Because of failures of human or hardware and even software package errors cloud information is related to information integrity. Several mechanisms have been proposed in order to allow both the data owners as well as the public auditors to audit cloud data integrity eciently without retrieving the entire data from the cloud servers. A Third Party Auditor (TPA) can perform integrity checking and also the identity of the signer on shared information is kept personal from them. During this project, we tend to solely investigate for auditing the integrity of shared information within the cloud with efficient user cancellation whereas still conserving identity privacy. we tend to additionally enhance this method, once any user change the value from table then we tend to analysis that value and automatically restored original value.

KEYWORDS*:* Cloud computing, Data security authorized auditing, Fine-grained dynamic data update, Third Party Auditor (TPA).

I. INTRODUCTION

The cloud computing is web based mostly laptop, shared computer code info and resources to world. Individuals will use this technology via their laptop computer, PC, mobile phones, etc. The mix of cloud computing and mobile computing is Mobile Cloud Computing. Currently a number of users stores their information on cloud. Thus security is a crucial factor in cloud computing, for making certain clients information is placed on the secure mode within the cloud. Information should not be taken by the third party, thus authentication of client becomes a compulsory task. Here the main issue authentication is mentioned. During this paper proposed data authentication to secure information of encryption algorithmic program with digital signature in local cloud server. If a user has uploaded the files on cloud server for sharing with multiple users, there ought to be a mechanism to verify the creator of the file. The authentication mechanism may help to verify the creator of the file.

Cryptographic technology is employed for the secure transaction and to protect the sensitive information. most typically three ways are used to offer security.

1. Private Key cryptography (Symmetric)

2. Public key cryptography (Asymmetric)

3. Hash Function

Symmetric cryptography use same key to each decryption and encryption. asymmetric cryptography use completely different key to encryption and decryption.

In this paper, DES cryptography technique is mentioned for data authentication. Digital Signatures is employed to verify the info, owner of the info. Digital signatures are fundamental in the present current circumstances to check the sender of documents originality. As a string of binary digits this digital signature presented in a PC. This signature is

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

PC utilizing an set of guidelines and parameters (calculation) such the personality of the individual marking the archive besides in light of the fact that the innovation of the information is checked. The signature is confirmed makes utilization of an public key that relates to (yet not indistinguishable, i.e. scientifically infeasible to see private key from public) the private key. With every client having an public/private key match, this can be a case of public key cryptography. Public keys, that are best-familiar with everyone, is utilized to confirm the signature of a client. The private key is not shared and is utilized in signature generation, which may exclusively be finished by the client. These signatures are utilized to identify unapproved alterations to data. Likewise, the receiver of a digitally signed file in demonstrating to an outsider that the record was so signed by the person it's identity asserted to be signed by. Which can be called non-repudiation, as the person who signed the record can't deny the signature at a later time.

A. Aims and Objectives:

In the proposed model aim and objective is to provide full security to the info hold on cloud storage. It is done by enhancing the level of privacy, confidentiality, authentication and incorporating the scheme of integrity. That makes alert to user for cases such as data integrity violation. To protect information against unauthorized access as well as security breaches many techniques of novel encryption and different mechanisms are going to be combined. Proposed model
implement in two phases. Primary phase is related to storing information on cloud storage securely. And second is related to accessing data from cloud.

II. REVIEW OF LITERATURE

Liming Fang et al., (2013) [1], in this paper author explained PEKS model that provides security against three attacks. These attacks are chosen keyword attack, chosen cipher attack and keyword guessing attack. Also this model protects from inside as well as outside enemy. Thus, important security ideas (IND-SCF-CKCA and IND-KGA) are given.

Nirmala et al., (2013) [2], creator clarified a strategy known as user authenticator. Based on this technique, firstly the info file is splited into equal pieces by info owner. After splitting Advanced Encryption Standard on every piece is performed. Once encryption is done, for each piece hash code is produced. After executing all steps, the encrypted report is hold on cloud. When downloading file, user has to send request to the cloud to produce hash code for that file. To confirm the integrity of info user has to check hash code with its hash code. Overall activities happen at user side and to produce hash code and to store encrypted information, cloud is employed.

Eman M. Mohamed et al., (2012) [8], in this paper author studied all techniques providing the security on cloud file. Eight encryption algorithms like AES, MARS, DES, 3DES, RC4, RC6, Two-fish and Blowfish are based on statistical testing (NIST) and Pseudo Random Range Generator (PRNG). To select any one of these algorithms one software is used which is on-demand security software. Encryption speed is tested to measure performance of algorithm. These eight algorithms are compared and this comparison is based on P-value and rejection rate.

Sherif El-etriby et al.,(2012) [7], in this paper, eight encryption algorithms are compared by an author. Compared algorithms are AES, DES, 3DES, RC4, RC6, Two-Fish and Blow-Fish. These algorithms are compared at PC as well as at Amazon EC2 cloud environment. The calculations are assessed according to the arbitrariness testing by utilizing NIST measurable testing in cloud environment. Pseudo Random range Generator (PRNG) is utilized to finish up the preeminent appropriate method.

PradeepBhosale et al., (2012) [6], this investigation in view of worldwide cloud, with a specific end goal to give a more secure distributed computing condition. Creator chipping away at 3D structure and advanced mark with RSA calculation. In this framework in view of the utilized 3D structure the customer initially select the parameters among

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

CIA and after that the advanced mark is made by utilizing MD5 calculation and after that the data is scrambled by making utilization of the RSA calculation and finally the figured information is put away on cloud condition.

G Jai Arul Jose et al., (2011) [12], in this paper, creator gives the security framework that gives verification, secrecy, and uprightness of client's data by association the distributed computing system. Additionally cluster load balancing, SSL over AES and secure session is implemented. Security display is separated into various layers.

Qin Liu et al., (2011) [14], R3 the time and quality principally based re-encryption system is proposed utilizing which cloud server can consequently re-encode the client data upheld its inner clock and oversees and guarantees the entrance control rightness.

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

Phase I (Data Storage Phase) :

All through this stage, client at first needs to login onto local cloud to validate character. This stage is again partitioned into subphases, for example, storage section selection and encryption stage, and integrity key generation.

a) Storage Section Selection and Encryption Phase : The primary advantage of this stage is that the cloud can offer the diverse levels of security to the clients as indicated by their own particular decision, it will give thoroughly secure capacity area utilizing encryption.

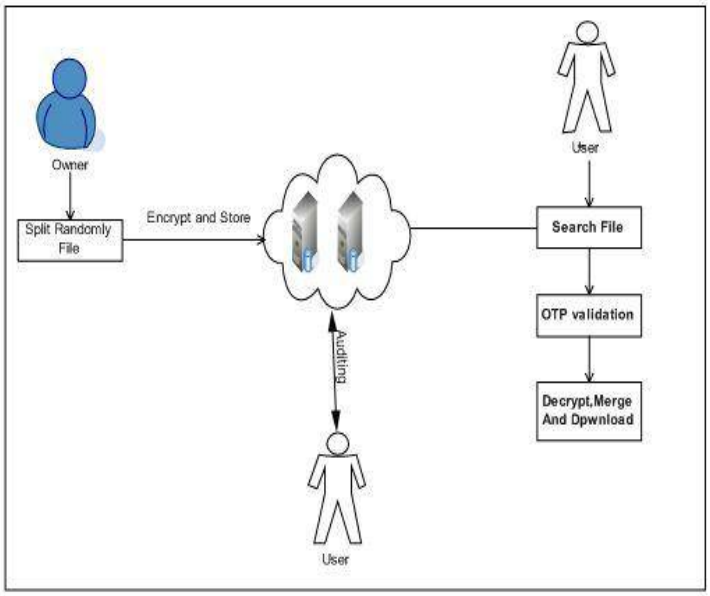

Fig. 1. System Architecture

Admin: They are responsible for granting access privileges to the users of the respective group. Admin has the main access permission for maintaining the files over cloud. Admin can navigate through the group as well. Admin can view the log details of the activities carried on the cloud file storage.

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

User: Every user needs to register with the corresponding group for getting access permission and signature key from the same. Using the signature key they can get the access permission. they can upload the files to cloud. User from same group can view the content of the file from cloud and make changes over it and can save them. Simultaneously they can download the files as well.

Third Party Auditor (TPA): TPA has the rights to validate the files which are available in the cloud. TPA is the respective authority for performing the verification of files which are uploaded by any user who are registered under a single group.

8. i=sp1,sp2,sp3;
9. Encryption decryption with AES
r=encsp1, encsp2, encsp3
w=decsp1, decsp2, decsp3
10. file downloading fd;
11. serfile from db server
12. if(fd==serfile)
13. Skey=send to user mail(otp).
Add ori=(sp1+sp2+sp3)
download the file.
Else
Cancel the file;
14. End;

IV. SYSTEM ANALYSIS

A. Algorithms:

1) Algorithm I AES: AES(advanced encryption standard).It is symmetric algorithm.It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128 bit /192 bit/256 bit input(0,1)

secret key(128 bit)+plain text(128 bit). Process:
10/12/14-rounds for-128 bit /192 bit/256 bit input Xor state block (i/p)
Final round:10,12,14

Each round consists:sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

2) Algorithm II Secure Erasure Coding: 1. Begin;

2. ow and pwd;

3. Based: = the privileges based on the entry system in the cloud computing
4. ownname =ow pwd=password

5. Then

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

6. If(skey==cfile)

7. Files upload i;

V. EXPERIMENT RESULT

In the result analysis of proposed system describe security of files with two tier system,

Result Graph for Encryption:-

In this,encrypt the files for the security purpose. So how many files AES encrypt with more security is shown in the below graph. It compares AES encryption Security.

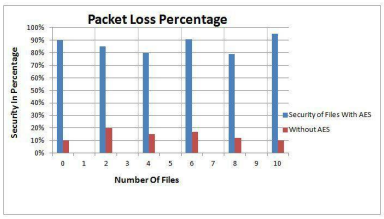

Fig. 2. Graph for security in percentage

TABLE I

PARAMETER VALUES WITH AES AND WITHOUT AES

With AES	Without AES
90%	10%
85%	20%
80%	15%
91%	17%
79%	12%
95%	10%

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

VI. SOFTWARE REQUIREMENT SPECIFICATION

The Introduction of software requirements specification provides an overview of all software used in Projects which used the operating system window 7,8,10. The Language used to implementation is java which required the JDK (Java SE Development kit) JDK have many version such as the 1.2,
1.3 and up to 1.7. Platform which used for JDK is eclipse, eclipse have lost of the version. To run the code in eclipse required the Server as the Apache tomcat 7.Data base used as the MYSQL version 5.

VII. CONCLUSION

This paper introduced a Data privacy has become extremely important in the Cloud environment. The issue of file auditing of data on networks has been summarized. Offers storage that is secure and easy to share across platforms. Data stored is highly secured using the cryptography algorithms and digital signatures. It integrates some new concepts like data security, storage optimality, file integrity and authentication access which are not present in the current system.

ACKNOWLEDGMENT

I want to precise my profound thanks to all who helped us directly or indirectly in creating this paper. Finally I want to give thanks to all or any our friends and well-wishers who supported us in finishing this paper with success. I am especially grateful to our guide Prof. Nilesh Sable Sir for his time to time, significantly required valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Liming Fang, Willy Susilo, ChunpengGe, and Jiandong Wang, ”Public Key Encryption With Keyword Search Secure Against Keyword Guessing Attacks Without Random Oracle”, Elsevier, pp. 221-241, 2013.
[2]V. Nirmala, R. K. Shivanadhan, and Dr. R. Shanmuga Lakshami, ”Data Confidentiality and Integrity Verification using User Authenticator scheme in Cloud”, International Conference on Green High Performance Computing, IEEE, pp. 1-5, 2013.
[2] Mr. Prashant Rewagad, and Ms. Yogita Pawar, ”Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, International Conference
on Communication Systems and Network Technologies, IEEE, 2013.
[4] MandeepKaur, and Manish Mahajan, ”Implementing Various Encryption Algorithms to Enhance The Data Security of Cloud in Cloud Computing”, International Journal of Computer Science Information Technology Volume: 2, pp. 831-835, 2012.
[5] AfnanUllah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, and KarimDjemame, ”Security Risks and their Management in Cloud Computing”, International Conference on Cloud Computing Technology and Science, IEEE, pp. 121-128, 2012.
[6] Pradeep Bhosale, Priyanka Deshmukh, Girish Dimbar, and Ashwini Deshpande, ”Enhancing Data Security in Cloud Computing Using 3D
[7] Framework Digital Signature with Encryption”, International Journal of Engineering Research Technology Volume: 1, Issue: 8, 2012.
[8] Sherif El-etriby, and Eman M. Mohamed, ”Modern Encryption Tech- niques for Cloud Computing”, ICCIT, pp. 800-805, 2012.
[9] Eman M. Mohamed, HatemS.Abdelkader, and Sherif EI-Etriby, ”En- hanced Data Security Model for Cloud Computing”, International Conference on Informatics and Systems, 2012.
Mark D. Ryan, ”Cloud computing security: The Scientific Challenge, and A Survey of Solutions”, Elsevier, pp. 1-6, 2012.
[10] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, WeiweiJia, and Yunlu Chen, ”Security and Privacy for Storage and Computation in Cloud Computing”, Elsevier, pp. 1-16, 2012.
[11] Miao Zhou, Yi Mu, Willy Susilo, Jun Yan, LijuDong, ”Privacy En-hanced Data Outsourcing in the Cloud”, Elsevier Journal of Network and Computer Applications, pp. 1367-1373, 2012.
[12] G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom, ”Implemen-tation of Data Security in Cloud Computing”, International Journal of P2P Network Trends and Technology Volume: 1, Issue: 1, pp. 18-22, 2011.
[13]AmanjotKaur, and ManishaBhardwaj, ”Hybrid Encryption for Cloud Database Security”, International Journal of Engineering Science Advanced Technology Volume: 2, Issue: 3, pp. 737-741, 2011.
[14]Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, ”Reliable Re-encryption in Unreliable Clouds”, IEEE, pp. 1-5, 2011.