PUBLIC AUDITING METHOD FOR SHARED DATA IN CLOUD WHICH ENSURE DATA PRIVACY AND INTEGRITY

[1]Ms.Kirtee G. Chaudhari , [2]Prof.Sonali A. Patil ,

[1]Student, Computer Engineering, BSIOTR,Wagholi,Pune,Maharashtra,India.
[2]Professor,Computer Engineering, BSIOTR,Wagholi,Pune,Maharashtra,India

Abstract : Cloud storage becomes one of critical services, because on the cloud users can easily modify and share data with other users. However, to preserve the integrity and confidentiality of shared cloud data is becoming difficult. To ensure the integrity of the shared data, some methods have been proposed to allow public verifiers to efficiently audit data integrity without retrieving the entire user information from cloud. In the existing scheme of public auditing for the integrity of shared data may reveal data owners sensitive information to the third party auditor. In this paper, we propose a new public auditing method for shared data in cloud which ensure data privacy and integrity. This mechanism is able to perform auditing tasks for numerous users. This proposed auditing method makes use of AES algorithm for encryption and decryption process. Nowadays, survey has been worked to enhance the cloud computing progress towards the internet services. Security and privacy problems are becoming key responsibility with the developing popularity of cloud network services.

Index Terms- Data Integrity, Data Confidentiality, Security.

I.INTRODUCTION

Cloud computing is a computing that depend on shared resources rather than having local servers or devices to handle applications. In most simple explanation, cloud computing is taking cloud services and moving them outside an organizations firewall. Applications, storage and other services are accessed via the web. The services are delivered and applicable for the Internet and are cashed by the cloud customer on an as-essential or pay-per-use business model. In a public auditing method for shared data in cloud which ensure data privacy and integrity, we maintain integrity and confidentiality of shared data.

Our scheme is capable to perform auditing task for numerous users. Public verifier is capable to audit shared data integrity instead of fetching the whole information of users. This proposed auditing method makes use of AES algorithm for encryption and decryption process.

EXISTING SYSTEM:

The existing mechanism a new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifiers. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy

LIMITATIONS:

- As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.
- They do not perform the multiple auditing tasks in simultaneously.
- Loss of information .
- Does not provide any privacy for private information.
- Authentication time takes too long.

PROPOSED SYSTEM:

In this paper, we propose a new public auditing method for shared data in cloud which ensure data privacy and integrity. This mechanism is able to perform auditing tasks for numerous users. This proposed auditing scheme makes use of AES algorithm for encryption and decryption process. Here we have also used SMTP protocol for mail transfer.

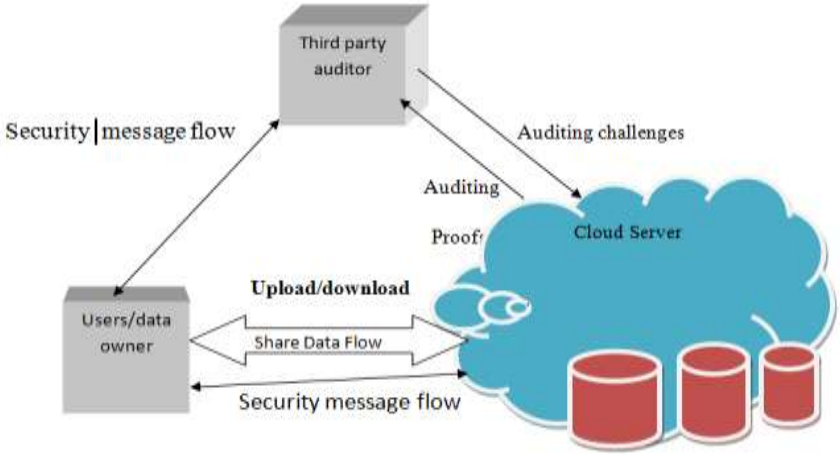


Fig:Proposed System

ADVANTAGES:

- The proposed system can perform auditing tasks for numerous users.
- They improve the efficiency of verification for auditing tasks.
- High security provide for file sharing.

II. LITERATURE SURVEY

1.Privacy Preserving Public Auditing For Secure Cloud Storage, Cong Wang, Sherman S,M. Chow, Qjan Wang, Kui Ren, Wenjing Lou. We apply the homomorphism direct authenticator and random masking to insurance that the TPA cannot gain awareness of information details saved on the cloud server during the effective auditing process, we can remove the load of cloud users from the costly auditing tasks, also users may worry about their outsourced information discharge. It is provably secure and highly efficient. These increasing tasks can be hectic and bulky of individual auditing.

2.A Secure and Dynamic Multi keyword Ranked Search Scheme Over Encrypted Cloud Data, Zhihua Xia, Xinhui Wang, Xingming Sun and Qian Wang

The database users are protected against privacy violation remotely stored encrypted database model is effective and safe ranked multi-keyword search. Effectiveness of the scheme can be increase by use of symmetric-key encryption The ranking scheme determines to be effective to recover more compatible documents matching to submitted search terms.

3.Public Auditing For Shared Data With Efficient User Revocation In The Cloud, Boyang Wang, Baochun Li, Hui Li

In cloud a public auditing method for shared information with effective user cancellation .Cancelled user using proxy re-signature. The semi-trusted cloud permitted to resign sections that were signed .Important computation and communication resources during user cancellation saved by group. Cancelled user should no longer be able to access and change shared information .Existing users verify the integrity of the entire data with the public key.

4..Auditing For Distributed Storage System,Anh Le,Athina Markopoulou,Alexandros G Dimakis

Server is a safe and effective in RDC method for network coding-based distributed storage systems .When faced with data corruption, replay, and pollution attacks used ensure data remains intact by RDC-NC scheme .The RDC-NC method is inexpensive for both clients and servers.

5.Oruta:Privacy Preserving Public Auditing For Shared Data In Cloud, Boyang Wang , Baochun Li ,Hui Li

Oruta, the TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. We exploit ring signatures to compute the verification information needed to audit the integrity of shared data. The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.

III. MATHEMATICAL MODEL

Let S be the system object it consist of Following Where S= I, P, O S denoted the System which Consists of the following,

I = Input

P = Process

O = Output

1. Input, I =U,F,CL

U=u1,u2,u3,..un that is users can be infinite.

F=f1,f2,f3,..fn and files can be infinite.

CL=Capability List

2. Process, P= P1, P2, P3, P4, P5 P1 = Process is carried out to ensure data Confidentiality DO and CSP and, authentication of DO and CSP. P2 = Process which DO and apply after a new file Creation in respect. P3 = Process ensures secure communication of data Between user. P4 = This process includes threshold cryptography technique for decryption of users file. P5 = This process is carried out to handle User

3. Output, O = Success, Fail

_ Success = User can decrypt the file if he has the proper access right as well as key part of threshold number of users.

_ Fail = User cannot decrypt the file if he does not have

proper access right or key part of less users than the threshold number of users.

IV. ALGORITHM

_ Advanced Encryption Standard (AES):

_ Input: Data

_ Output: Encrypted data
_ Step 1: Key Expansion: Using Rijndaels key schedule round keys are derived from the cipher key.
_ Step 2: First Round
1. Add Round Key: using bitwise XOR each byte of the state is combined with the round key.
_ Step 3:Rounds
1. Sub Bytes a non-continuous substitution step where every byte is replaced with another according to a lookup table.
2. Shift Rows a exchange step where every row of the state is moved periodically a particular steps.
3. Mix Columns a combining operation which operates on the columns of the state, integrating the four bytes in every column.
4. Add Round Key
_ Step 4:Final Round (no Mix Columns).
1. Sub Bytes
2. Shift Rows
3. Add Round Key

V. SYSTEM ARCHITECTURE

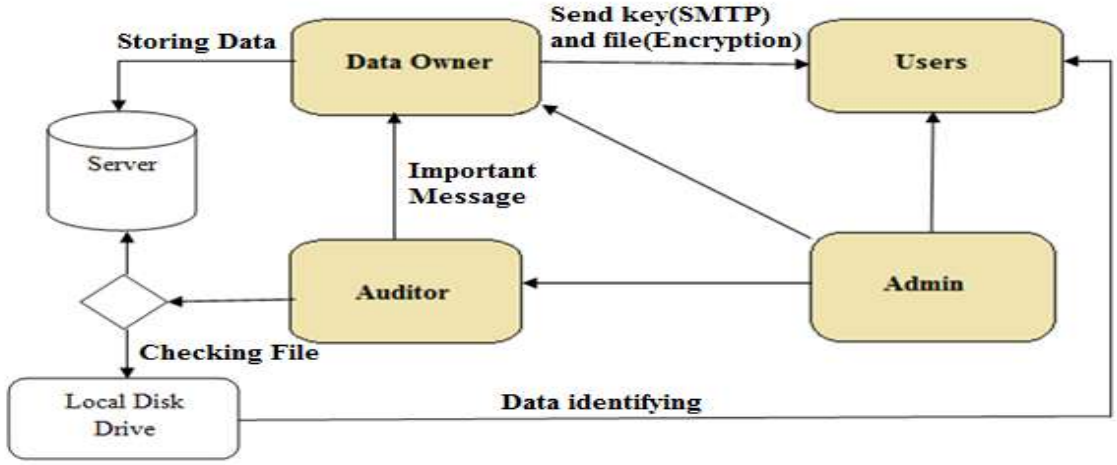


Fig: System Architecture

The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. A public verifier is able to audit shared data integrity without retrieving the entire data of user from cloud. There are main three modules i.e. data owner, data user, pubic auditor. First the data owner creates the data on cloud and then data user use this data after downloading from cloud. Auditor checks the integrity of shared data without retrieving all the details of users on cloud.

VI. MODULE DETAILS

- DATA OWNER: Data owner first make registration .At the time of registration data owner provide some personal details and sixteen character long key which is used for encryption and decryption purpose. After successful registration data owner upload data on cloud. Data in encrypted form will get stored on cloud.

- DATA USER: Data user first make registration. At the time of registration data owner provide personal details and email id so that the data owner will send the key on register email. After registering and selecting particular group, data owner can download a file.

- AUDITOR: After registering with the system data auditor is able to audit the data. Auditor checks the integrity of the shared data. Auditor ensures that there is integrity and data privacy of shared data in cloud.

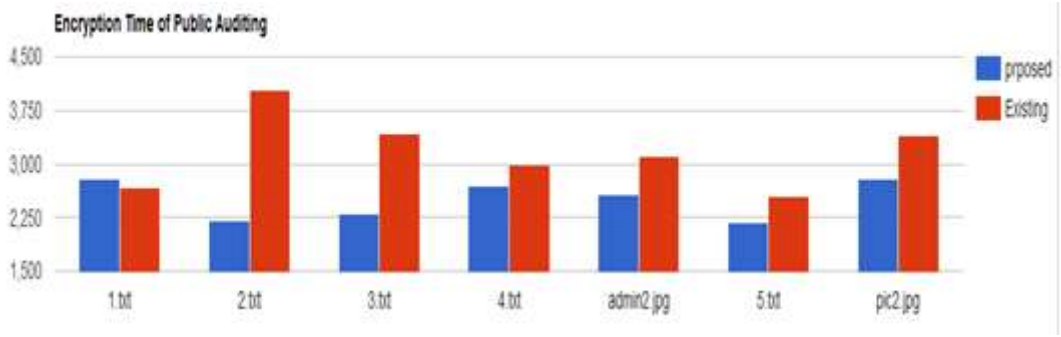
VII. OBSERVATION

Table I show a high-level comparison between our scheme and existing mechanism. To our best knowledge, this paper represents an effective privacy-preserving public auditing method for shared data in the cloud which ensure data privacy and integrity.

TABLE I
COMPARISON WITH EXISTING MECHANISM

	Existing System (PDP)	Proposed System
Public Auditing	Yes	Yes
Data Privacy	No	Yes
Identity Privacy	Yes	Yes
Authorized Auditing	Yes	Yes
User Revocation	No	Yes

VIII. RESULT



The encryption time required for public auditing method for shared data in cloud which ensure data privacy and integrity is less as compared to the existing system .The communication and computational costs of our scheme is small and acceptable. The proposed system ensure the data privacy and integrity in cloud.

IX . CONCLUSION

The proposed system provides a solution for privacy and integrity problem of the shared data in the cloud. The perfect solution is a public auditing method for shared data in cloud which ensure data privacy and integrity. Here the public verifier has the capacity to check shared data integrity without retrieving the whole data of cloud users.. In future will be work on how to avoid re-computation introduced by dynamic groups while preserving identity privacy from the public verifier during the process of public auditing on shared data.

ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully. I am especially grateful to our guide Prof.Sonali A. Patil and Head of Department of Computer Engineering Dr.G.M.Bhandari, PG Coordinator Dr.A.C.Lomte madam for their time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement, the paper would not have been completed on time. Also I would like to thanks our Principal Dr.T.K.Nagaraj for allowing us to pursue project work.

REFERENCES

[1] Anmin Fu , Shui Yu , Yuqing Zhang, Huaqun Wang, and Chanying Huang " A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" IEEE transaction on Big Data,2017

[2]D. Fernandes, L. Soares, J. Gomes, et al, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 12, no. 2, pp. 113-170, 2014.

[3] W. Hsien, C. Yang, and M. Hwang, "A survey of public auditing for secure data storage in cloud computing," International Journal of Network Security, vol.18, no.1, pp. 133 142, 2016.

[4] J. Yu, K. Ren, C. Wang, et al, "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2015.

[5] Q. Wang, C. Wang, K. Ren, et al, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[6] S. Yu, "Big privacy: challenges and opportunities of privacy study in the age of big data," IEEE Access, vol. 4, no. 6, pp. 2751-2763, 2016.

[7] C. Wang, Q. Wang, K. Ren, et al, "Privacy-preserving public auditing for data storage security in cloud computing," Proceedings of IEEE INFOCOM, pp. 1-9, 2010.

[8] B. Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2014.

[9] B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," Applied Cryptography and Network Security. Springer BerlinHeidelberg, pp. 507-525, 2012.

[10] B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing for shared cloud data supporting group dynamics," Proceedings of IEEE ICC, pp. 1946-1950, 2013.

[11] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," Proceedings of IEEE INFOCOM, pp. 2904- 2912, 2013.

[12] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol.8, no.1, pp. 92-106, 2015.

[13] C. Liu, J. Chen, L. Yang, et al, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.9, pp.
2234-2244, 2014.

[14] H. Wang, and Y. Zhang, "On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.1, pp. 264-267, 2014.

[15] L. Huang, G. Zhang, and A. Fu, "Privacy-preserving public auditing for dynamic group based on hierarchical tree," Journal of Computer Research and Development, vol.53, no.10, pp. 2334-2342, 2016.

[16] Y. Yu, J. Ni, M. Au, et al, "Comments on a public auditing mechanism for shared cloud data service," IEEE Transactions on Services Computing, vol.8, no.6, pp. 998-999 2015.

[17] Kirti D. Patil, Sonali A. Patil, " Pseudonym Generation with Combining the Identity based and Attribute based Encryption with Outsourced Revocation in Cloud Computing ", International Journal of Innovative Research in Computer and Communication Engineering & Technology (IJIRCCE) Volume 4 Issue 5, May 2016 3800 ISSN: 2320 9801

[18] Kirti D. Patil, Sonali A. Patil, " Pseudonym Generation with Combining the Identity based and Attribute based Encryption with Outsourced Revocation in Cloud Computing ", International Journal of Science and Research (IJSR) Volume Issue , June 2016 ISSN: 2319-7064