INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Public Integrity Auditing with Multi user Modifications

Kolachina. Amrutha
Sathyabama Institute of Science and Technology,
Chennai, Taml Nadu

Dr. Prayala Shyry
Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu

ABSTRACT

Cloud Computing has visualized as the next-generation architecture of IT Enterprise. A cloud storage system, consisting of a collection of storage servers, provides long time storage services over the internet. Storing data in third party's cloud system causes serious concern over the data secrecy. In, this paper our main aim is, we allow the third party auditor on behalf of the cloud client, to verify the integrity of dynamic data that is stored in the cloud. The most general forms of data dynamic are modifications, insertion, and deletion. To, give the more efficiency in handling the multi-users the ring signature is used by the privacy-preserving mechanism. When the data is stored in the cloud it has an only certain time limit to be present in cloud storage to overcome this time limit process we use hashing technique, this makes the data to be stored in a long period of time, by key generation process. And, also we use MD5algorithm for uploading the data and encrypted in hexadecimal form.

Keywords: *Cloud Computing, Hashing, Key Generation, Ring Signature, Encryption, MD5 Algorithm.*

1. INTRODUCTION

Cloud Computing moves the application software and databases to the centralized large data centers. The main objective of our concept is an administrator is the prior permission for any users or data creators. Data creators will create the data and forms group members after the approval from administrator only the user can access. In, this while the file is uploading to the server public auditor, we use the MD5 (Message Digest) algorithm for encrypting the file to 16-bit hexadecimal form by this the security of the data is increased. While uploading the data to server public auditor there will be traffic in data transferring process in mean while the third party an unauthorized may interrupt the data which is transferring this will be taken care by admin through implementing ring signature by privacy-preserving mechanism this send an alert message by using SMTP protocol, therefore, it decreases the leakage of data. Data creator can use the operations of insertion, delete and modification in mean time any leakage occur that taken care by the administrator.

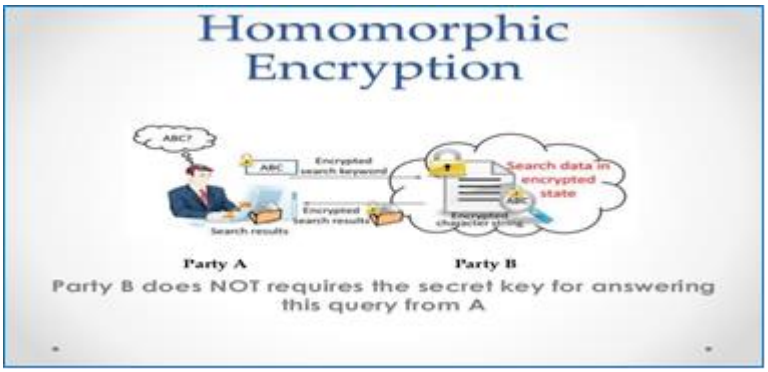
As the file uploads the data is encrypted into 16-bit secret key this 16-bit secret key, then the file is distributed into 4*4 matrix form that is compressed to 32-bit hexadecimal form to store the data a long period of time without any time period limitations, by using a hashing algorithm. In this Hashing algorithm, the key is generated to 64bit to 128 bit. The services of cloud computing are not limited to archive or backup. These prior works on ensuring the data integrity often lack the support of either public audit ability or dynamic data operations, but this paper achieves both the concepts. Extensive security and performance analysis are shown in the proposed schemes are highly efficient and probably secure.

2. RELATED WORKS

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls. The management of the data may not fully trust worthy. Actually, In the extension system the AES(advanced encryption algorithm) is present this has 64 bit and 8-bit key, while this is using it, has only limited time if that limited time is crossed the data won't be in the cloud it is corrupted or gone anywhere. By, this there are many drawbacks that we are overcoming using Hash (SHA) algorithm this keeps the data long period. And there is triple DES algorithm also there but when achieving towards the leakage in process of traffic it is not done properly. So, in the proposing system, we are using ring signatures that give the alert message when any interruption of the unauthorized user using that message is identified through SMTP protocol (simple mail transfer protocol).

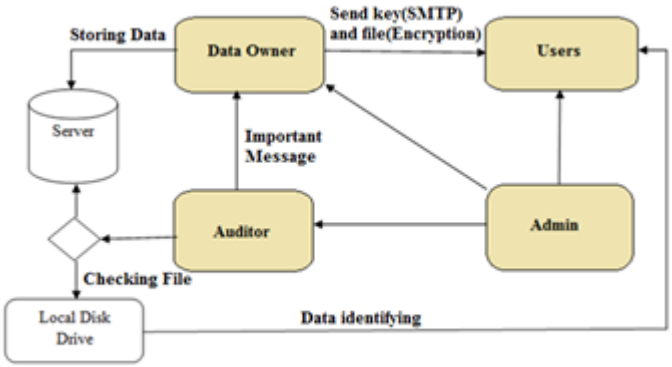
A. Homomorphic Encryption

This allows the computation of the cipher text, generating an encrypted file, decrypted and checking whether it matches with the plain text. Here the secret key which is created by the administrator and itself creates a data if that is matches or not is checked bye the homomorphic encryption. This encryption helps us in identifying whether any corruption is there or not. The files that which are all stored in Data Base are encrypted and decrypted by this encryption process cypher text to plain text.



B. Architecture.

BLOCK DIAGRAM:



Description of block diagram:

In this architecture the data owner, users, auditor, and admin are present. Data owner can create the data like this they can form group members also that data is stored in the server that server is audited by the auditor and kept in a local disk drive in mean while admin will approve the data owner then only the data owner can access. The user now directly uses the data that is stored on the local disk drive. When the Approval is done from the admin the data owner receives a message through SMTP protocol and the file is encrypted by usingMD5 algorithm in giving the 16bit secret key. If any important message is to be delivered means the admin can deliver directly to the data owner. Here the deletion and insertion can be done directly. If any user is not useful anymore the admin can revocate or delete directly.

C. Used Software Components:

Operating System: Windows

Coding Language: Java (JDK 1.7)

Data Base: SQL server

Net Beans IDE (8.0.2)

TomCat/GlassFish

D. Used Hardware Components:

System : Pentium IV 2.4GHz

Hard Disk : 40GB

Floppy Drive : 1.44 Mb

Monitor : 15 VGA colour

Ram : 512 Mb

3. CONCLUSION

By doing this process the data will be stored long period of time and the leakage of data is avoided. This also prohibits the unauthorized user involving in the data transferring phase. And also loss of packages are decreased. This is the advanced stage of auditing in both the public and also in data dynamic nature. The key generated in the hash increases the data storage capacity.

4. REFERENCES

[1] Nu˜ nez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis,"Cryptography goes to the cloud," in Secure and Trust Computing, Data Management, and Applicat., 2011, pp. 190–197.
[2] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE]
[3] Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data", IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, Feb. 2016.
[4] Q. Jiang, J. Ma, F. Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services", IEEE Syst. J.
[5] Nu˜ nez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis,"Cryptography goes to the cloud," in Secure and Trust Computing, Data Management, and Application.
[6] Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud (Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE)
[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson D.Song, "Provable data possession at untrusted stores,"in Proc. 14th ACM conf. Compu. Commun. Security (CCS), 2007, pp 598–609.
[8] G. Ateniese, A. Faonio, and S. Kamara, "Leakage-resilient identification
schemes from zero-knowledge proofs of storage," in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–328
[9] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalableand efficient provable data possession," in Proc. 4th Int. Conf.Secure and Privacy in Commun. Netw. (SecureComm), 2008, pp. 1–10.
[10] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in Proc. Theory Cryptography Conf. (TCC),2009, pp. 109–127.,

