Third Party Auditing (TPA) For Secure Cloud Storage With Secret Sharing Algorithm

SHEETAL THITE[1],
M TECH,Computer Engineering,
BVDUCOE,
Pune,india

Prof. S.S.DHOTRE
Associate Professor,Department of Computer Engineering
BVDUCOE,
Pune,india

Abstract:

A scalable data storage service can be offered at a much lower cost by cloud storage providers. Users can be used cloud storage to remotely store there data. It will be helpful for the user to freed from extra load of storage space for data storage and manipulation of data but cloud storage also leads to invite the risk of no longer having physical possession of the data theft. Necessary efforts has been taken to build trust amongst use using different approaches for data security on cloud. Our main approach is also one step towards reducing this risk. In this approach access based privacy preserving authentication protocol (APPAP) is used. It will definitely address above privacy issue for cloud sharing and storage.

Keywords: *Cloud Storage, Shared Data, Privacy Preserving, Secret Sharing, Authentication, Third Party Auditor(TPA).*

I. INTRODUCTION

Cloud computing is the latest technological innovative architecture for enterprises and individual. Even in a short span of time elapsed since its inception it has gained immense popularity due to immense benefits it offers to its users. In the IT perspective there are many aspects where cloud provides its services like Service On Demand, Uninterrupted Data access via Cloud storage services, Pricing based on usage, quick resource expansion [6].On Demand service feature has many benefits: freedom from burden of storage space and management, data access anywhere anytime, Relief from the cost of hardware and software maintenance. As is always with many advantages there are few concerns also raised by users, the major concern or the risk the user is exposed to is security of the outsourced data, because the data is stored on remote cloud servers the availability and integrity of the data is not always assured [8]. This issue if addressed will eventually increase the users trust and confidence of its usage. To address the above mentioned anomalies our approach of Access Controlled based Data Security in Cloud environment has been devised and discussed in this paper.

Contribution:

The Contribution of this paper are:

1. Shared access authority by author access granting mechanism.
2. Permission Level based access control to realize that user can have access at which level
3. Effective Data Encryption mechanism so that security of the data can be preserved.
4. Intermediate MD5 re-encryption is applied by the cloud server to provide secured data sharing among the multiple users.

Organization:
The remaining of the paper talks about the analysis of the existing systems and there pro's and Con's. Our approach discussed in detail and the problem statement along with the evolution of the algorithm.

II. EXISTING SYSTEM

Cong Wang has proposed public audit ability for cloud storage. To illustrate his approach he has developed a cloud storage mechanism which is secured by the implementation of public auditing via privacy preserving and designed a Third Party Auditor which will audit multiple users in parallel with enhanced performance. but due to random masking at the cloud server and auditing task overhead may have an impact on the efficiency of the cloud performance.

Earlier Researcher's has proposed a public auditing based privacy preserving protocol for secure cloud storage based on unpadded RSA based public auditing. This approach is better in terms of data privacy and public audit ability, though this approach seems better but as claimed by author the full fledged implementation is yet to be complete.

III. SYSTEM FLOW

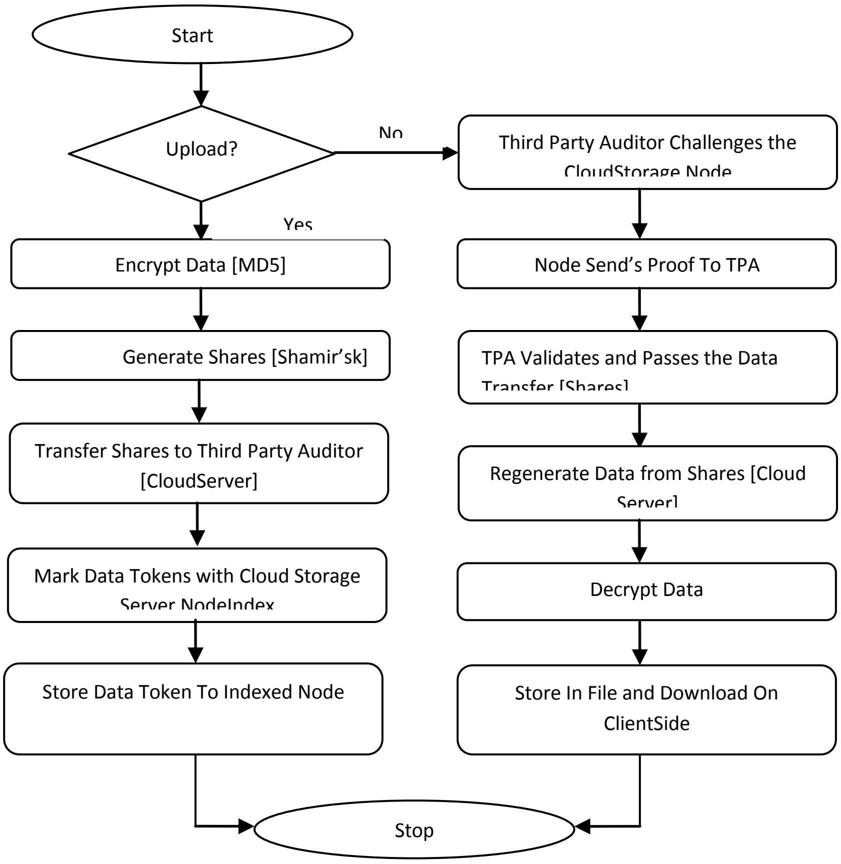
Start
Upload?
No
Yes
Encrypt Data [MD5]
Generate Shares [Shamir'sk]
Transfer Shares to Third Party Auditor [CloudServer]
Mark Data Tokens with Cloud Storage Server NodeIndex
Store Data Token To Indexed Node
Third Party Auditor Challenges the CloudStorage Node
Node Send's Proof To TPA
TPA Validates and Passes the Data Transfer [Shares]
Regenerate Data from Shares [Cloud Server]
Decrypt Data
Store In File and Download On ClientSide
Stop

Figure 1 System Flow

IV. PROPOSED SYSTEM

Third Party Auditor (TPA) mechanism thus the user is able to shared the data while having the facility to allow/ deny access along with the read write permission to a single user an group of users. The data which is shared by user is encrypted and secret shares are generated and some but not all secret shares are stored on the distributed cloud Environment. Thus TPA has the complete data to authenticate the integrity of the data. Thus as per our approach the TPA will be able to do the auditing without asking for the local copy of the data which in turn will result in less communication and computational load.

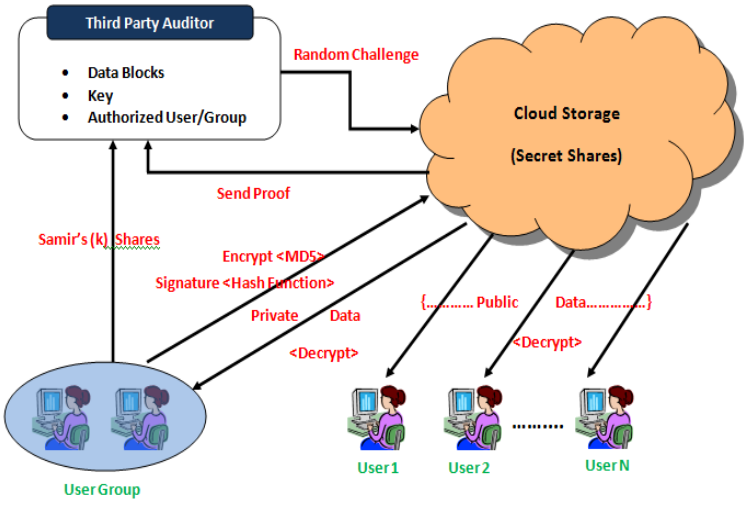

Figure 2 Proposed SystemArchitecture

Algorithm:
Secret Share Generation using Shamir's Secret Sharing

Let the secret data be a value D. An algorithm defines a k-out-of-n threshold secret sharing scheme, if it computes D(s) = [d1,d2,….,dn] and the following conditions hold

Correctness: D can be determined by any k shares from d1,d2,…, dn and there exists an algorithm S0 that efficiently computes D from these k shares.
Privacy: having access to any one of the k shares from d1,d2,….,dn gives no information about the value of D, i.e., the probability distribution of k isto 1 shares is independent of D.

Steps To Regenerate Original Data:-

Suppose we want to use (K,N) threshold scheme to share our secret D where K should be less than or equal to N.
Choose at random (k-1) coefficients d1,d2,d3…dk-1 , and let D be the a0

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{k-1}{}^{k-1}$$

Construct N points
(if(i)) where i=1,2…..N

Given any subset of K of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=D , which is the secret message reconstructed.

MD5

MD5 is a hash table based encryption algorithm. It consists of five steps as described below:
1. Appending Padding Bits: The original message is taken as input and then it is extended so that its length becomes equal to 448, modulo 512 bit. The rules for the extension are as below:

- Initially original message is always padded with one bit "1".
- Then zero or more bits "0" are added to bring the length of the message up to 64 bits a bit lesser than a multiple of 512.

2. Appending Length: The 64 bits appending happens at the end of the extended message to show the length of the original message in bytes. Rules of appending length are:

- The original message length in bytes is converted into binary of 64 bits. In case of overflow, the low-order 64 bits are used.
- Separate the 64-bit length into 2 words of 32 bits each.
- The high order word is appended after the low order word is appended.

3. MD Buffer Initialization: Because MD5 algorithm needs a 128-bit buffer with a specific initial value. The rules of initializing buffer are:

- The buffer is separated into 4 words (32 bits each), named as W1, W2, W3, and W4.
- Word W1 is initialized to: 0x67452301.
- Word W2 is initialized to: 0xEFCDAB89.
- Word W3 is initialized to: 0x98BADCFE.
- Word W4 is initialized to: 0x10325476.

4. Processing Message in 512-bit Blocks: This is one of the main step of MD 5 algorithm, which converts padded and appended message into 512 block size. For each input block, 4 rounds of operations are performed with 16 operations in each round.
5. Output: The contents in buffer words W1, W2, W3, W4 are returned in sequence with low-order byte first.

V. EVALUATION AND ANALYSIS

As a proof of enhancement in security and data storage and retrieval correctness we considered the two users scenario where we consider that both the users belong to same group. Beyond this we have also demonstrated the assurance of security of bulk auditing for the TPA in multiple user environment. We focus our result evaluation on the below discussed three parameters,

Storage and Retrieval Correctness
Security in form of privacy preservation and authentication
System Performance.

Storage And Retrieval Correctness

The classic cloud storage has two components
End User: It is the web browser which access cloud interface storage by using host name and port id
Cloud Storage **Server:** It is the server which contains cloud exchange, cloud coordinator and multiple data centers. Cloud exchange waits for End User connection request. When it receives a connection request it accepts connection request at same time it also creates a client request handler thread to handle another client request. Client thread to handle client request methods- Constructor Method

is Initialize client Thread to store socket and storage Manager Reference in data members. Run Method will read a request first then process the request and send a response to the cloud user. In the process request first it will read command, domain name and password from client request packet. In datacenter to check a domain is registered or not if not registered then send a error massage in a response to the cloud client else do operation according to request.

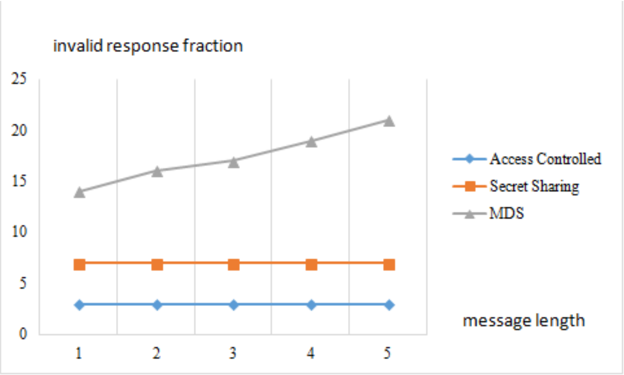

Figure 3 Storage and Retrieval Correctness

Security In Form Of Privacy

The three step approach of Encryption, Secret Sharing and User Group Authentication is used to preserve the privacy more effectively. The existing systems used to work individually on the approaches i.e. an encryption system only encrypts the data whereas we have seen many user group authentication systems where data can be shared amongst trusted users only. The approach implemented here is utilize the beneficial aspects of these approaches and combine to enhance the privacy preserving manifolds.

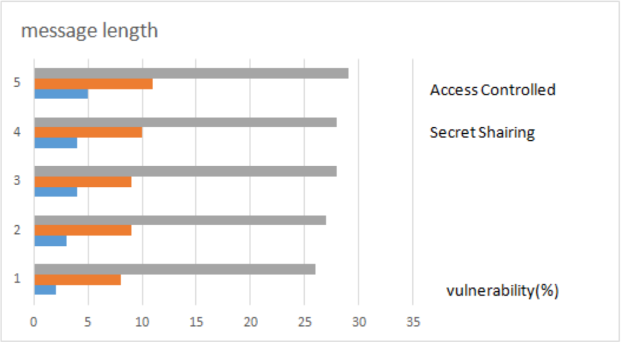

Figure 4 Storage and Retrieval Correctness

System Performance

In the approach implemented here we have tried to share the load of computation between the cloud server and the client system. So the task of encryption and secret share creation has been performed on the client side and storage and proof generation and will be done on the Cloud server side. It has two fold benefits firstly it will reduce the risk of data theft while data transfer from client to server and also reduce the computational load on server.

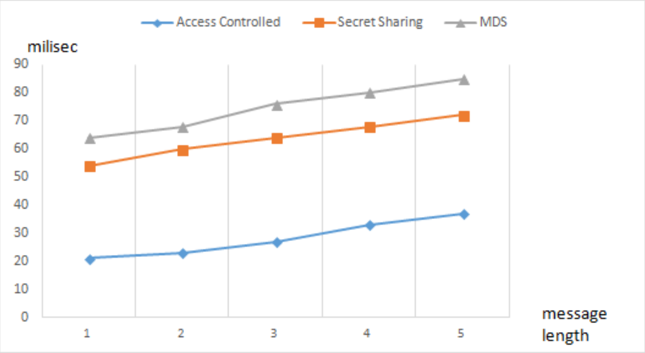

Figure 5 System performance

VI. CONCLUSION

Considering the evaluation results we conclude that our approach has enhanced the privacy preserving feature of Cloud Storage environment, which will enhance the user trust on the Cloud Storage service providers and thus the usage of Cloud will also be improved with a better user experience on two aspects i.e. Performance and Data Security. Our system has been developed and tested on homogeneous cloud environment so the scope of such system for heterogeneous cloud is the area for future research.

REFERENCES

[1] Aten,2011 R. Curtmola , G. Ateniese, R. Burns, J. Herring, L. Kissner, Z. Peterson, and D. Song. In ACM CCS, 598–609, 2007.Provable data possession at untrusted stores.

[2] Bowe,2009 K.D. Bowers, A. Juels & A. Oprea (2009A), Proc. ACM Conf. Computer and Comm. Security (CCS ’09), 187–198.—HAIL: A High-Availability and Integrity Layer for Cloud Storage,

[3] Boya,2014 Boyang Wang; Baochun Li; Hui Li, Cloud Computing, IEEE Transactions on: 43 - 56 Volume: 2, Issue: 1, Jan.-March 2014. "Oruta: privacy-preserving public auditing for shared data in the cloud".

[4] Fern,2014 Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014).. International Journal of Information Security, 13(2), 113-170.Security issues in cloud environments: a survey.

[5] Kaus,2013 Md Kausar Alam, Sharmila Banu K, International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153, An Approach Secret Sharing Algorithm Cloud Computing Security over Single to Multi Clouds.

[6] Mell,2009 P. Mell and T. Grance, ," Referenced on June. 3rd, 2009."Draft NIST working definition of cloud computing

[7] Nupo,2013 Miss. Nupoor M. Yawale., Prof V. B. Gadichha P R Patil COET..Volume 3, Issue 11, November 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm

[8] Vara,2014 Varampati Deepa, P. Jyotheeswari & Vikram Neerugatti., The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 2, No. 5, July 2014, A Privacy-Preserving Unpadded RSA based-Third Party Auditing Protocol for Cloud Storage Secure.

[9] Wang ,2012 Wang, C.,Wang, Q., Ren, K., Cao, N., & Lou, W. (2012)., IEEE Transactions on, 5(2), 220-232, Toward secure and dependable storage services in cloud computing. Services Computing.

[10] Wang,2011 Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011, IEEE Transactions on, 22(5), 847-859,). Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems.

[11] Wang,2013 Wang, Cong, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Computers, IEEE Transactions on 62, no. 2 (2013): 362-375, "Privacy-preserving public auditing for secure cloud storage."

[12] Jans,2011 Jansen, W., & Grance, T. (2011).. NIST special publication, 800, 144, "Guidelines on security and privacy in public cloud computing"

[13] Sheet,2015 sheetal Thite & S.S.Dhotre., volume 5,Issue 4, April 2015, ISSN:2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering, " Access Controlled Data Security in Cloud Environment".

[14] http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

[15] http://php.net/manual/en/function.md5.php