Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.187 – 191

SURVEY ARTICLE

Survey Paper on Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud

Lokesh.P.Chaudhari[1], Prof. Umesh.B.Chavan[2]

[1]Department of Information Technology, Walchand College of Engineering, Sangli, India

[2]Department of Information Technology, Walchand College of Engineering, Sangli, India

[1]lokeshc7490@gmail.com,[2]umesh.chavan@rediffmail.com

Abstract-- Cloud computing is growing now days, all physical systems are going to be history in coming years as cloud computing provides the virtualize framework of all i.e. software, hardware etc. The one of the most efficient use of cloud is data storage on cloud server on pay as you go scheme. But as its good to hear there are some challenging aspects behind this cloud data storage as per end users perspective. How end users know their data is secure on cloud server? How they satisfied that the data is not tampered and successfully updated after performing some operation over it?

Here the Trusted Third Party auditor comes in picture and using auditing framework he satisfy end users that there data is secure over server and successfully updated. So in this paper efficient secure auditing algorithm is designed and also extended to dynamic auditing.

Keywords – Cloud Computing; Data storage; Efficient Privacy Preserving Auditing; Storage Auditing; Secure Dynamic Auditing.

I. INTRODUCTION

Cloud computing is the growing field now a days. The virtualize platform it provides help to reduce the cost as well as make the effective utilization of the hardware as well as software. Data storage is the main most desirable aspect of the cloud computing, but it comes with some security challenges too. The end users store their data on cloud server are always in worry that either their data stored is secure or not? As the data stored is large enough so users can't check its integrity periodically. Sometimes cloud service providers may be behave unhonestly and delete customers data Or they fail to make changes on the data which updated by the users frequently.

So to overcome these challenges the Trusted Third Party Auditor plays the vital role on behalf of customers. As they assure to customers that the data hosted on the server is secure. They provide the unbiased result also the TPA is same like the government institute so they are trustworthy and it holds the capabilities to convince cloud service provider as well data owner.TPA provides more easier and affordable way for users to their storage correctness in cloud. It is also helpful for the cloud service providers to improve their cloud based service platform. In other way we can say auditing scheme play a significant role in establishment of secure cloud platform in users mind and increase the cloud economy ,where users accesses the risk and apply their trust in the cloud to store data more precisely.

II. BACKGROUND

A. Basic Concepts

Three main entities in cloud environment include:

- Cloud Service Provider: It provides data storage service as well as cloud servers with significant resources.

• Data Owner: Owners keep their own data to the cloud server and access them when needed. They rely on the cloud for data computation.
• Third party auditor: An optional TPA is trusted to assess and expose risk of cloud storage services on behalf of the user's open request. It has expertise capabilities to convince both CSP as well as Data Owner.
Fig.1 shows the basics of cloud computing.

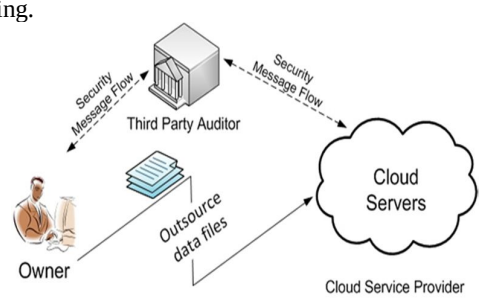

Fig.1. Basics of Cloud

B. Characteristics of auditing protocols

While designing this data integrity checking protocol, they must satisfy some requirements:[3]

- Highly private: The TPA should not gain knowledge of the original user data during the auditing process.
- Data dynamic: The clients must be able to perform operations on data files like insert, alter and delete while maintaining data correctness.
- Open verifiability: Anyone, not just the clients, must be allowed to verify the integrity of data.
- Block free verification: Challenged file blocks should not be retrieved by the verifier during verification process.
- No restriction of queries: The verifier may be allowed to use unlimited number of queries in the challenge-response protocol for data verification.

C. What are the challenges in the cloud data storage security are:

- Snooping: Snooping is to peep into others private data. It is a best way to send and retrieve the data over a secure transmission line.
- Cloud Authentication: The clients can obtain others authorization and may delete the files. Hence it is necessary to protect one's unique authorization. The unauthorized clients must not be log in to others account and delete the data.
- Key Management: The cryptographic keys have to be managed in the cloud environment but this key management must be user friendly.
- Data Leakage: Data leakage occurs when it is transmitted between the user and the cloud server. The best way is to encrypt the data from owner's side.
- Performance: An durable security approach is necessary for encrypting and decrypting the files to and from the cloud but it should keep the user's performance integral.

III. RELATED WORK

In this section we first review some existing related works carried out in security aspects of cloud data storage. Security issue is very important in cloud there are many techniques available so here is review of all these. Data security is the major challenge in the cloud computing as user's data reside in the servers which are remotely situated and far away beyond the knowledge of end-users. The data store may be highly private data eg. Any personal information, financial data, health records which may cause a severe loss to the data owner if this disclose. So data security comes as the highest priority issue [2]. In [3] they put one trusted third party auditing on behalf of data owner for verification, in which they describes three network entities i.e. Data owner which is end user, Data storage server which is managed by cloud service provider and Third party auditor which is maintained the trust to owner about his data In this case TPA having public key, it is act with only trusted server, so data privacy remains the major issue here. Paper [4] is distributed in 2 phases phase 1 : Owner calculate the MAC on each partitioned file block whichever going to store in cloud server. Transfers the file blocks &codes information to cloud server and shares the key with TPA. At the time of confirmation auditing phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding MACs to verify the correctness of the data file. This scheme holds some drawback too i.e. if TPA is not trustworthy then data may lead to outside world, i.e. if both CSP as well TPA handshakes then

owner don't have option other than failure. Phase 2: In this phase, User uses s keys and computes the MAC for blocks and user shares the keys and MAC with TPA. During Audit, TPA gives a key (one of the secret keys) to CSP and requests MACs for the blocks. TPA compares with the MACs at the TPA. Improvement from operations, i.e., it only allows very basic block operations with limited functionality, and block insertions cannot be supported Scheme 1: TPA doesn't see the data, preserves privacy. Drawback: a key can be used once, this scheme just helpless for dynamic data operations[9].In (PDP) [5] ensures the accession of data files on untrusted storages. It uses a RSA based scheme authentication for auditing data, but this model leaks the data to external world and hence it violate the privacy preserving approach. When SSL Authentication Protocol (SAP) was employed to cloud, it becomes very complex. As an alternative to SAP, proposed a new authentication protocol based on identity which is based on corresponding signature and encryption schemes [6]. Signature and encryption schemes are proposed to achieve security in cloud storage phenomena. When comparing performance, authentication protocol based on identity is very weightless and more efficient and also weightless protocol for client side. To store and maintain client's data, existence of multiple cloud service providers are considered in which a cooperative provable data possession (CPDP) is used to check the integrity and availability of stored data [7].The data owner processes the file using a secret key and sends the file with some verification tags to the CSP. Then the CSP is requested to verify the integrity of data. The procedure for verification is
The file is processed with a secret key to generate a set of procedure for verification and is transferred to the CSP, by using the verification procedure, the files are audited for its integrity.

For this proposed scheme the three different main entities are used those are as follows:

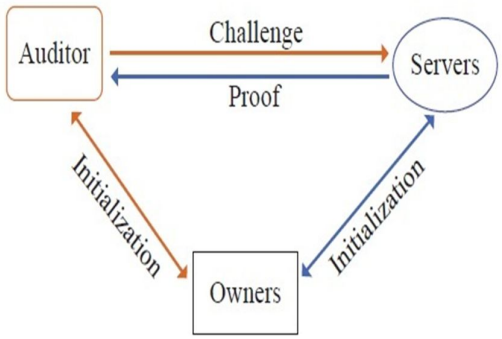

Fig.2. Basic Flow of Auditing Framework.

Functionality of Entities:
1.Owner : Owner keeps his data to cloud server generate set of keys.
2. Server: Data stored on the server with the respective FID
3. Auditor: Owner shares set of keys to auditor, once owner curious about the file stored on the server it simply as auditor to verify the integrity of the data by challenging the server.
An auditing scheme consists of five algorithms (Keygen, TagGen, Challenge, Proof and Verify).

- KeyGen: key generation algorithm that is run by the user to setup the scheme by generating the set of keys.
- TagGen: used by the user to generate verification metadata, which may consist of signatures or other information used for auditing
- Challenge: run by the auditor on the CSP to check the verifiability of the file stores on the server as per owner order.
- Proof: run by the cloud server to generate a proof of data storage correctness
- Verify: run by the TPA to audit the proof from the cloud server by checking the actual hash and calculated hash by server.

IV. PROPOSED PRIVACY AUDITING PROTOCOL

So as to overcome the data privacy problem from the auditor as well as server here we proposed some advanced algorithm. In this scheme we proposed the KeyGen algorithm which simply generates set of keys TagGen algorithm is there to generate the secret tag key to each data component. Chall(M) algorithm generates the encrypted data set of data block. Proposed auditing system can be constructed from the above auditing scheme in two phases, key generation and Audit.

Phase 1:

In this case the keys are generated by client and send these keys i.e. hash keys to the server along with the encrypted data. Once these keys are stored with server this keys are send to the TPA. Now both the server as well as Auditor has the set of keys.

Phase 2:

This is the actual working phase of the algorithm, in this phase the two ways communication established, i.e. Challenge and Proof In this case, the owner ask auditor to check the integrity of his data whichever stored on the cloud server by sending some FID of the file to the auditor. Once the auditor got task he conducts the auditing as follows:

I. The auditor runs the challenge algorithm. The auditor runs the challenge algorithm Chall to generate the challenge C for all the data blocks in the data component and sends them to the server.

II. Upon receiving the challenge C from the auditor, the server runs the prove algorithm Prove to generate the proof P which contain Tag proof and Data proof and sends it back to the auditor.

III. When the auditor receives the proof P from the server, it runs the verification algorithm Verify to check the correctness of P and extract the auditing result. The auditor then sends the auditing result to the owner. If the result is true, the owner is convinced that its data is correctly stored on the server and it may choose to delete the local version of the data.

In this phase sampling auditing may carried out. In which auditor can ask for any random challenge to server and server will respond periodically. Auditor maintains table for this periodic checking and send it to auditor periodically and ensure him that data is secure. In this case if data is tampered then auditor tracks it easily and convey message to client.

V. PROPOSED DYNAMIC AUDITING PROTOCOL

In cloud data storage system, the data owners perform updating frequently. As per the definition of the auditing protocol, they should fulfil to handle the dynamic data and static data. But the dynamic operations make auditing protocol insecure, as many attacks server can make to track the data or to tamper the data as it is easier to crack update operation. Server may undergoes the following attacks which are

The CSP may not update correctly the clients data on the server and may use the flesh data to pass the auditing or

The client updates the data to the current version, the server may get enough information from the dynamic operations to track the data tag. If the server could track the data tag, it can use any data and its data tag to auditing and make fool to auditor easily

To overcome this drawback in this proposed scheme the Index Table is maintained to keep the detailed information of the data stored. This table consists, the Index denotes the current FID of data block, data component. The original block number of data block and current version number of data block, the timestamp is used for generating the data tag. This Table is created by the owner during the initialization phase and the auditor manage this table afterwards. When the owner completes the dynamic data operations, it sends an update message to the auditor for updating the table which is with auditor. Once whole table is updated with auditor the auditor sends the result to the owner for the confirmation that the data on the server and the all information in Table on the auditor side are updated successfully.

This scheme is also distributed in 3 phases

1. Data update:
   In this phase the insert, delete or update operations are carried out and the index table update successfully, the insertion operation inserts a new block number new version number and keeps it in the i'th position in the index table, similar operations carried out in deletion as well as modify case, i.e. i'th location is deleted and new version of data block and tag values are generated respectively. This new data bocks and tag values are send to server and stored.
2. Index update:
   As this messages received to the auditor, it update the index table as per the updation carried out.
3. Proof of updation:
   Once the auditor updated its index table he ask for the challenge of any data block to the server and then server generate proof using this challenge and data block and reply proof to the auditor. Once auditor receive this proof it checks the hash values, if they match then he assure that the data is updated successfully and send this information to the owner.

VI. CONCLUSION

Cloud Computing increases the ease of usage any service by giving access through any kind of internet connection. As with these increased ease of usage followed drawbacks too. Data security is a key issue for cloud storage and is to be considered very important. To ensure that the risks of data security have been mitigated a variety of techniques that may be used in order to achieve security. This paper has addressed some secure approaches for overcoming the issues in security on

untrusted data servers in cloud computing. This paper categories the methodologies in the literature as auditability schemes, dynamic auditing. This approach is fully sophisticated to give a secure and dynamic auditing framework by considering all pros and cons to achieve highly security of data stored on cloud server that overcomes all the other privacy concerns.

ACKNOWLEDGMENT

We express our sincere thanks to all the authors, whose papers in the area of cloud computing security and auditability aspect which are published in various conference proceedings and journals.

REFERENCES

[1] Kan Yang, XiaohuaJia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS* 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," *Proc. 17th Int'l Workshop Quality of Service (IWQoS '09)*, pp. 1-9, July 2009.

[3] [C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage*," IEEE Trans. Computers, preprint*, 2012, doi:10.1109/TC.2011.245.

[4] [Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22,no. 5, pp. 847-859, 2011.

[5] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. 2007, October. Provable data possession at untrusted stores.*InProceedings of the 14th ACM conference on Computer and communications security* (pp. 598-609).ACM.

[6] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, 3-42.

[7] Zhiguo Wan, Jun'eliu and Robert H.Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing", *IEEE transactions on information forensics and security*, vol.7, no.2, April 2012, pp.743-754.

[8] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," *IEEE Vol 24, no. 4,* pp. 19–24, 2010.

[9] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in *HotOS, G. C. Hunt, Ed.*USENIX Association, 2007.

[10] Arjun Kumar, Byung Gook Lee, HoonJaeLee "Secure Storage and Access of Data in Cloud Computing" *2Department of Computer and Information Engineering Dongseo University, Busan*, 617-716, Korea.

