ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Third party auditing techniques in cloud data storage

R.K.Saranya[1], A.Vidhya[1], D.Bhaskar[2]
1. Assistant Professor, Department of CSE, Jeppiaar Engineering College, Chennai
2. Assistant Professor, Department of CSE, Indira Institute of Engineering & Technology, Chennai
***Corresponding Author: saranya.rks@gmail.com**

ABSTRACT

Cloud computing is a new trend in computing environment. Computing infrastructure based on this model is viewed as a cloud. By using this cloud, the data owner can access and store their application on demand from anywhere in the world. Cloud is the internet based technology, where the storage and computational resources are provided as a resource service. But the data owner's application will be placed in the remote places. There is a chance of accessing those applications by the unknown users. This paper deals with the problem of security issues while outsourcing and access the data in the cloud. Before outsourcing the data owner's application in the cloud, the identity based authentication process will be done between the data owner and the cloud server. The secure verification process will be done periodically to avoid the data modification, deletion and insertion. For this verification the Third Party Auditor (TPA) is used.

KEYWORDS: Cloud Computing, Identity Based verification, TPA, Security

1. INTRODUCTION

Cloud computing is a new trend in computing environment, here it is dynamically scalable and virtualized resources are provided as a services over the medium called internet. So many Cloud Computing service providers are there, for example Amazon, Google, Microsoft, Sales force etc.

Nowadays Cloud Computing is act as a major part of all IT Enterprise. Application software and databases will be transferred to the centralized large data centers, there the management of the data and services may not be fully trustworthy. To avoid this problem auditing concept was used. For doing multiple auditing task effectively. Third Party Auditing (TPA) is introduced to verify the integrity of dynamic data stored. For block tag authentication Merkle Hash Tree construction is used for dynamic data storage and for auditing a technique called bilinear aggregate signature is used.

By using this TPA we can achieve integrity, confidentiality, integrity etc. Outsourcing of data in the cloud become a critical task, as the proposed system deals with the problem of security issues while outsourcing and accessing the data in the cloud. Before outsourcing the data in the cloud, the identity based authentication process among the data owner and cloud server. After outsourcing the data, when the original service provider access the data in the cloud the secure verification process to avoid the malicious cloud service provider auditing task is delegated to TPA auditor, who will do the auditing and find the mischievous servers these all described in this paper .

The rest of the paper is ordered as follows. Section II discusses some related work in security methods for data storage in cloud. Section III presents the problem definition and the overview of Frame work of TPA. Section IV illustrates about the details of Proposed Framework. Section V describes the experimental results. Sections VI provide the conclusion.

Problem definition: This section describes about the Third Party Auditing (TPA) frame work to verify the integrity of dynamic data storage systems.

Problem Definition: The definition of the problem can be distinct as a detailed and operational description of the differences between the existing situation and the desired situation.

In existing system the dynamic data auditing performed by the user using the erasure code to verify the storage correctness and mischievous server. Existing system deals with the problem of Auditing and dynamic data operation done by user in un- trusted cloud servers in a distributed cloud storage system. Existing scheme auditing is performed by the data owner not only keeps load of data storage also the time and the computational resources to audit the cloud storage system.

Another major concern is the security issue of dynamic data operations for public audit services. When the cloud service provider accesses the data in the cloud, there is chance for the illegal users to hack the data on behalf of original cloud service provider. When the data owner outsource the data in the cloud , there is possible for the individuality attack to hack the original data Auditing is performed by the data owner, data owner couldn't able to do audit periodically and finding the mischievous servers are time consumption.

TPA Frame Work: TPA is used to verify the integrity, confidentiality and availability in dynamic cloud data storage. The frame work for TPA is showed in Fig.1. Once data owner uploaded the file in the cloud server the TPA is checking the reliability of the uploaded file at any time. At first the TPA challenges the Cloud Service Provider (CSP) for the verification process. TPA will send the block indices to randomly challenge the cloud. The cloud computes the signature for the specified block. The signature of file block should equivalent to the corresponding tokens of file block. The verifier TPA checks whether the reply is correct and auditing is performed among the CSP and TPA.

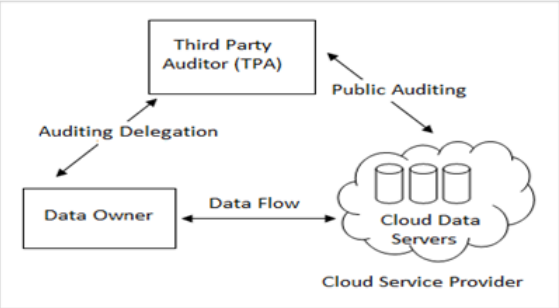

Fig.1.Third Party Frame Work

2. MATERIALS AND METHODS

Proposed frame work: The main goal is to deals with the problem of security issues while outsourcing and accessing the data in the cloud. In Fig.2, it describes that the data owner and cloud server will negotiate session key to establish secure data processing for identity based authentication. Then the data owner uploads their file to the cloud data center. The uploaded files will be divided into blocks and the token for each block will be generated by homomorphic token algorithm. At the same time these tokens are stored in TPA. Auditing takes place for some portion of file from cloud data center using the token randomly by TPA. The auditing message will be produced to the data owner. Here the dynamic data operations such as Insert, Update and Delete can also be performed.

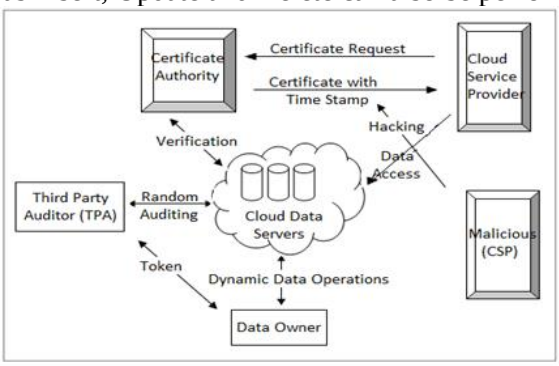

Fig.2.Proposed frame work architecture

Requirements:

Data owner: Data owner is one of the entities which contain the data to be stored in the cloud storage system which is provided by the cloud service provider the data owner may be an individual user or a small organisation.

Cloud service provider: The cloud service provider (CSP) which provides the various cloud services in our approach CSP provides the data storage space and computational resources.

Cloud servers: The collection of mainframe systems or server which is owned and managed by the cloud service provider (CSP) which provides the computational resources.

Certificate authority: The certificate authority is one of the entities in the architecture which provides a valid certificate during the identity management.

Trusted third party auditor: The trusted third party auditor is one of the entities who has versatile, skilled, computational resources that users may not have and provides the audit service on behalf of the user.

Identity Based Authentication: At first the user sends the request to cloud server for the authentication process, the request contains the user address. After receiving the certification request, the cloud generates the random number and sends it to the user. Next user sends the public key to the server, and then cloud sends the random number with the user public key with the received random number user computes the token and sends it to the cloud server. Finally the server verifies that the generated random number and public key is equal to the token that is generated by the user. If the validity is true cloud server start sending the session key otherwise the communication will be blocked.

Outsourcing in the Cloud: In the proposed system, Data owner outsource the data in the cloud. The data owner split the files into number of blocks and it's multiply with the parity vectors. Using homomorphic encryption algorithm each file block is encrypted. Then encrypted file is send to the cloud servers and the token is send to the third party auditor.

Periodic Auditing Using Third Party: Once data owner uploaded the file in the cloud. The TPA is checking the integrity of the uploaded file at any time. At first the TPA challenges the CSP for the verification process. TPA will send the block indices to randomly challenge the cloud. The cloud computes the signature for the specified block. The signature of file block should match the corresponding tokens of file block. The verifier TPA checks whether the reply is correct and auditing is performed among the CSP and TPA.

Error Localization and Correctness Verification: In order to eliminate the errors in the storage system, the data error localization has to construct. By integrating the correctness verification and error localization could identify the *mischievous servers*. Every time the TPA challenges the cloud by sending block indices. From the response values of cloud servers in each challenge determines the correctness of the distributed storage, TPA check whether the received values provides valid code word, if it doesn't return the valid code word, there exist file corruptions in file. Once the error has been found next task is to identify which server is misbehaved, TPA send the response to each server one by one and find mischievous server.

Algorithm: Correctness Verification and Error Localization:

```
1. procedure CHALLENGE(i)
2.        Recompute αi= fkchal (i) and k(i)prp from KPRP ;
3.        Send {αi, k(i)prp} to all the cloud servers;
4.        Receive from servers:
          {Ri(j)= ∑'q=1αqi*G(j)[ fk(i)prp (q)]|£ j £ n}
5.        for (j←m+1,n) do
6.             R(j)← R(j)_ ∑'q=1fkj(sIq,j). αqi,Iq=fkprp(i) (q)
7.        end for
8.        if ((Ri(1) , . . .;Ri(m)·P== Ri(M+1),...., Ri(n)) then
9.           Accept and ready for the next challenge.
10.       else
11.            for (j←1; n) do
12.                 if (Ri(j) != vi(j) then
13.                      return server j is misbehaving.
14.                 end if
15.            end for
16.       end if
17. end procedure
```

File Error Recovery: The TPA sends the queries to the servers to send back blocks of the r rows specified in the challenge. TPA will regenerate the correct blocks by using erasure correction, if the number of identified mischievous servers is less than threshold value. The newly recovered block is again send to the mischievous servers to maintain the correctness of storage.

Dynamic Data Operations: Dynamic data operations are handled among the data owner and cloud server. The dynamic operations are handled in the blocks. Data owner send the request to the server to modify the file. Upon receiving the modification information, cloud server modifies the file block. Then the cloud server calls the Update, Delete and Insert operations to modify the file. Afterwards the server sends the proof of operation to the client.

Mischievous Attack: When the cloud service provider accesses the data in the cloud, it has to get the certificate from the certificate authority. An attacker may interrupt messages during the verification of a service provider with the certificate authority, and reply the messages in order to deception as a genuine service provider.

3. RESULTS AND DISCUSSION

Fig.3 represents Total Requests (the number of URIs requested from the user's application every second, including dynamic, static, and cached requests) and Total Errors (the number of errors generated by the user's application every second). Fig.4 represents the average number of milliseconds taken for the user's application to service a request (latency measure), including only dynamic requests. Includes the time it takes to process the request, but not the time it takes to deliver the request to the client. Fig.5 represents Sent (the number of bytes sent by your application every second, summed across all requests) and Received (the number of bytes that are received by your application every second, summed across all requests). Fig.6 represents Total CPU utilization (the amount of CPU mega cycles your application uses every second) and API Calls CPU (the amount of CPU megacycles your application uses every second to call Google APIs).

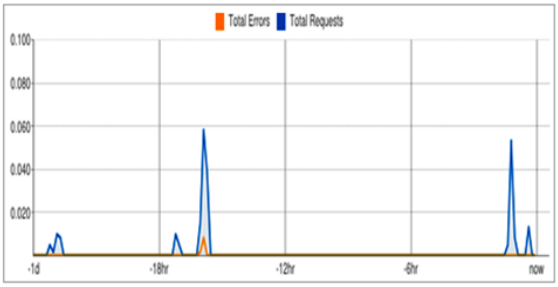

Fig.3.Summary based on total hits and total miss

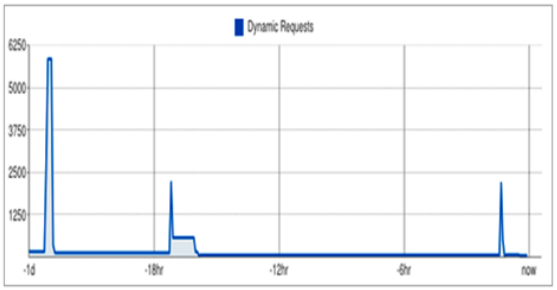

Fig.4.Dynamic request latency per day

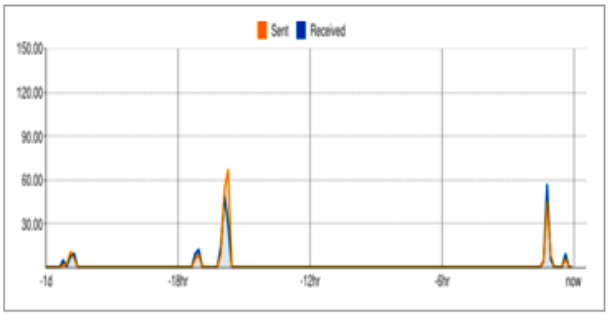

Fig.5.Network traffic per day

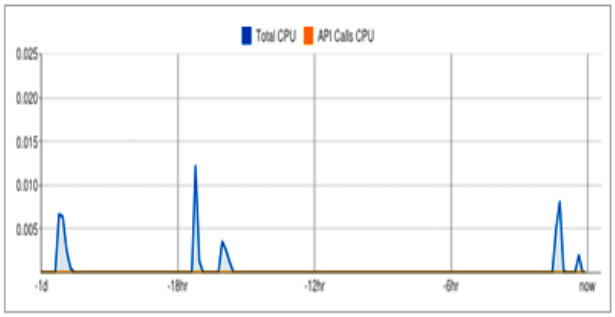

Fig.6.CPU utilization per day

4. CONCLUSION

Outsourcing user's or enterprise data in cloud has become critical task to perform business operations and vital for businesses to sustain in market and their competitive advantages. Maintaining security in cloud outsourcing is important for maintaining the growth of cloud technology and various cloud services. To achieve the assurances of cloud data integrity and data availability and enforce the quality of dependable cloud storage service for users, the proposed provides an effective, bendable and distributed scheme with explicit dynamic data operation support, which includes block update, delete, and insert data blocks.

Thus proposed scheme provides the secure outsourcing services by enabling periodic auditing using a trusted third party auditor and dynamic operations. Also the verification process provided for the cloud service provider to access the data in the cloud. Hence the malicious cloud service providers or malicious user are getting highlighted and removed from the cloud system. It provides identity based authentication service during the data owner trying to access the cloud server for data outsourcing. The dynamic data operations are performed by the data owner in the cloud itself.

REFERENCES

Bowers KD, Juels A, and Oprea A, Proofs of Retrievability: Theory and Implementation, Report 2008/175, Cryptology ePrint Archive, 2008.

Ren K, Wang C and Wang Q, Security Challenges for the Public Cloud, IEEE Internet Computing, 16(1),2012, 69-73.

Shacham H and Waters B, Compact Proofs of Retrievability, Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), 2008, 90-107.

Sundareswaran S, Anna C Squicciarini, Dan Lin, Ensuring Distributed Accountability for Data Sharing in the Cloud, IEEE Dependable and Secure Computing, 9(4), 2012.

Wang C, Wang Q, Ren K and Lou W, Toward Secure and Dependable Storage Services in Cloud Computing, IEEE Services Computing, 5(2), 2012.

Wang Q, Wang C, Ren K, Lou W, Li J, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Trans. Parallel and Distributed Systems, 22(5), 2011, 847-859.

Yu S, Wang C, Ren K, and Lou W, Achieving secure, scalable, and fine-grained data access control in cloud computing, IEEE INFOCOM'10, 2010.