ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

A Framework renders Data integrity issue and Bandwidth allocation over in Cloud

Mrs. V. Kavitha Chandrakanth, Mrs. P. Jamuna

***Abstract*— Cloud Computing is a technology where users can remotely store their data into the cloud environment so as to have the on-demand applications and services from the common pool of computing resources. By this, users can be relieved from the burden of local data storage and maintenance. However maintaining data integrity over Cloud environment is a very challenging task. Our proposed public auditability technique for cloud data security is of significant importance so that users can route to an external audit party to check the data integrity of outsourced data when it is needed. In this paper we make use of the public key based homomorphic authenticator with random mask method to achieve the privacy public auditability for data storage security in cloud and also with the fair share algorithm we are maintaining fair network bandwidth allocation. Our proposed public auditability and fair share technique achieves high security, performance, and also provide less communication and computation overhead.**

.

Index Terms—Public auditing, Third Party Auditor, Fair share, homomorphic authenticator, random mask

I. INTRODUCTION

Cloud computing is the emerging technology with the web users. As the name implies the users can access the information anywhere at any time. The advantage is that users can access that related article from where on earth with any device that has right to use the internet. Cloud Computing has been envision as the next-generation structural design of IT endeavor due to its extended list of extraordinary advantages in the IT history: On-demand self-service, location independent source pooling, ubiquitous network access, location independent source pooling, rapid resource elasticity, [3]. As an unruly technology with deep implications, Cloud Computing is transforming the nature of how businesses make use of information technology. One elementary aspect of this paradigm shifting is that information is being centralized or outsourced into Cloud. This can help cloud business to function more smoothly because anyone who can connect to the web and cloud users can work on documents, access software, and store data. The Cloud environment can be classified into four types are

1. Public Cloud – This type of cloud can be accessed by any subscriber and can access to the cloud network resources.
2. Private Cloud – A separate cloud environment is set up for the particular group or business organization and the users can access the resources within their group.
3. Community Cloud - A community cloud can be shared among two or more business organization that have like cloud requirements.
4. Hybrid Cloud – This type of cloud is essentially a blend of at least two clouds environment, where the Clouds comprise of public, private, or community

To firmly introduce an effective entity in cloud is Third Party Auditor (TPA) and it should meet the two important requirements: 1) TPA should provide efficient audit over in cloud without demanding the local copy of data, and should not introduce any additional burden to the user. 2) The Third Party Audit (TPA) should not bring any vulnerability towards data privacy

From the users' point of view includes both individuals and IT enterprises, storing the information remotely into the cloud environment which brings interesting advantages like relief from the storage management burden, worldwide information access with autonomous geographical location, and it avoids the initial expenses on software, hardware, personnel maintenances etc [4]. Briefly, even though outsourcing information into the cloud environment is economically attractive for the cost and complication of huge data storage, it does not provide any assurance on data integrity and availability. If it not properly addressed, it might obstruct the victorious employment of the cloud architecture. Whereas the benefits of using cloud environment are indisputable due to its opaqueness of the Cloud environment, as part of administrative entity the inner process details of Cloud Service Providers (CSP) may not be identified by cloud users.

The correctness of the information in the cloud environment is being laid at threat due to some following reasons. First, though the infrastructures under the cloud environment are more powerful and trustworthy than private computing devices, they are still meeting the huge range of both internal and external threats for data integrity [5][8]. Secondly, there exist several motivations for cloud service providers (CSP) to act disloyally towards the cloud users. For example reclaim the storage by discarding the related information that has not been or is not often accessed so as to preserve their reputation [9][11]. In recent times the perceptions of public auditability have been projected in the framework in order to ensure remotely stored data integrity under security models [9],[11], [2],[1]. Public auditability which allows an external entity, in addition to the client himself, to check the correctness of remotely stored information .However, most of them [9],[11] ,[2] do not hold the privacy protection of users .From the viewpoint of shielding information privacy, the users should

rely on TPA for the storage and the security of their information. The user doesn't want this auditing could bring in new vulnerabilities of illegal data leakage towards their information security [6].Data encryption before outsourcing [1] is the only method to ease this problem, but it is the complementary technique to the privacy-preserving auditing scheme to be proposed in this paper along with the scheme used for the maintenance of network bandwidth allocation.
Our complementary technique didn't solve the privacy data protecting completely but it can reduces the overhead to manage the encryption keys.

II. RELATED WORKS

In this section we have described various models in order to preserve privacy preserving public auditing .At first Ateniese et al. [9] have proposed "Provable Data Possession" (PDP) model to ensure the control of data files on unfaith storages. Their model used the RSA-based homomorphic authenticators for the auditing purpose on outsourced data and they have suggested a randomly sampling method for a few file blocks. On the other hand the public auditability demands the linear combination of sampled blocks which are exposed to the external auditor .But their model is not provably privacy preserving, when it is directly used and thus might disclose user information to the external auditor.

Juels et al. [1] have described a "Proof of Retrievability" (PoR) model, is used to ensure both retrievability and possession of data files on remote service systems where the model which contains error-correcting codes and spot-checking codes. However, this method works only with encrypted data and they have described a Merkle-tree construction for public Proof of Retrievability (PoR).

Shacham et al. [2], have proposed a new enhanced PoR model which is based on BLS signatures with complete proofs of security [1]. This enhanced model use verifiable homomorphic authenticators that are built based on BLS signatures which is similar to Ateniese et al. construction. Thus enhanced PoR model has achieved the public retrievability whereas their model also does not maintain privacy-preserving auditing. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in on-line burden to users when the keyed hashes are used up. In other related work,

Shah et al. [10],[6] have proposed a scheme which allows the TPA to hold data storage by encrypting the data first and it send a pre calculated symmetric-keyed hashes to the auditor. The auditor will check the integrity of data and server's possession of an earlier committed decryption key. This scheme works only for encrypted files and this scheme could bring an on line burden to the cloud user when the hash keyed function usage.

Ateniese et al. [7] have proposed a limited dynamic version PDP scheme so as to uses only symmetric key cryptography. On the other hand their protocol having the linear combination of sampled data blocks and it does not maintain privacy-preserving auditing on outsourced data. Existing systems had a public auditing scheme consists of the following algorithms are KeyGen, SigGen, GenProof, VerifyProof).KeyGen is a key generation algorithm which is used to setup the scheme by the user. SigGen is an algorithm used to generate verification metadata; it may include MAC or digital signatures. GenProof is an algorithm used to generate a proof of stored data by the cloud server in order to check its correctness, VerifyProof is an algorithm in order to audit that proof from the cloud server and its run by the TPA, protocol verifier is also used by the cloud server. Existing public auditing system is constructed in two phases are Setup phase and Audit phase where as the first phase does not provide privacy-preserving audit and also not a lightweight and the second scheme which renders the problem faced in the first one, but affect from adverted methodical demerits for public auditing like auditor statefulness and bounded usage, which might cause an additional burden to cloud users. Our proposed public auditing system achieves security and high performance.

III. PROPOSED WORK

Our Public auditability which allows an external entity, in addition to the client himself, to check the correctness of remotely stored information .However, most of them [9],[11], [2] do not hold the privacy protection of users .From the viewpoint of shielding information privacy, the users should rely on TPA for the storage and the security of their information. The user doesn't want this auditing could bring in new vulnerabilities of illegal data leakage towards their information security [6]. Fair-share is the scheme used for the maintenance of the network bandwidth allocation. Consider a cloud data storage service which has three different entities, as illustrated in fig. 1: the entities are cloud user (U), who has huge amount of information to be stored in the cloud, Cloud Server (CS), can be managed by Cloud Service Provider (CSP) to offer the data storage service and has considerable storage space and computation resources, Third Party Auditor (TPA), who has the capabilities to monitor and it provides cloud storage service security. Architecture of Cloud data storage device is illustrated in figure 1.

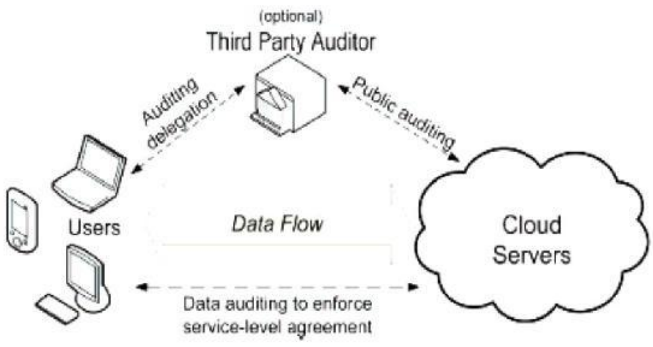

Figure1. Architecture of Cloud data storage device

A. Framework of Privacy –Preserving Public Auditing Technique

In our proposed system we adapt the framework for privacy-preserving public auditing .Usually a public auditing method which consists of the following algorithms are KeyGen, SigGen, GenProof, VerifyProof, protocol verifier). KeyGen is a key generation algorithm which is used to setup the scheme by the user. SigGen is an algorithm used to generate verification metadata; it may include MAC or digital signatures. GenProof is an algorithm used to generate a proof of stored data by the cloud server in order to check its correctness, VerifyProof is an algorithm in order to audit that proof from the cloud server and its run by the TPA, protocol verifier is also used by the cloud server.

Our proposed public auditing technique can be developed from the above auditing scheme. It includes three phases are Setup, Audit, Auto blocker

Setup: The cloud user initializes the public and private parameters by executing the KeyGen algorithm, and pre-processes the data by using the SigGen algorithm in order to create the verification metadata. The user can stores the data at the server side in cloud and delete its local copy of data, make publish the verification metadata to TPA for the purpose of auditing.

Audit: The TPA will generate an audit message to the cloud server in order to make sure that the cloud server has got the data properly or not. Then the cloud server will obtain a response message from stored data by executing GenProof algorithm. The TPA can verify the response message via VerifyProof algorithm with the use of verification metadata.

Auto Blocker: When the cloud user initializes the public and private parameters the system will verify all the particular parameters and validates, and this Auto Blocker blocks the unauthenticated cloud users. If the user is new one to access servers means the system prompts for security parameters, which is previously assigned by the system. In order to achieve privacy-preserving public auditing technique, we have distinctively integrated the Public key based homomorphic authenticator with random mask method. In our framework, the linear permutation of sampled blocks in server's response message is masked by a Pseudo Random Function (PRF). With this random mask, the TPA has all the required information to build up in a correct set of linear equations and with this we cannot obtain the data content owned by the user. In the meantime, owed to the algebraic property of the homomorphic authenticator, the correctness justification of the block-authenticator pairs will never be exaggerated by PRF.

B. Fair Share Algorithm

The bandwidth used in the cloud environment is the network bandwidth. Fair-share is the scheme is used for the preservation of the network bandwidth allocation.

The fair share "v" of the information flow can be defined as the highest flow of the resources without any collision in a given time. Consider two parameters collectively are throughput T and network weight C. The fair share value can be adjusted for a specific time interval Δ. The fair share value is updated when the aggregate of throughput T and network weight C is equivalent then the data can be processes. When there is difference between throughput and fair share v divided by the fair share value lies between the random number 0 and 1then the information process can be dropped .Thus fairness can be achieved among the network bandwidth.

```
1   UpdateFairShare()
2     Once every Δ units of time do
3       if T > 0.7C
4         v ← 0.9v + 0.1(C − T)
5       else
6         v ← 0.9v + 0.1(C)
7     enddo

8   PacketArrival()
9       if R < (t_i − v)/v
10          DropPacket
```

Pseudocode for Fare Share Algorithm

IV. CONCLUSION

In this paper, our proposed privacy-preserving public auditing framework for outsourced data security have used the public key based homomorphic authenticator and random mask technique to assure the TPA for effective auditing process by without keeping any local copy of data and also eliminate the cloud users burden also it provide less expensive auditing task. Our proposed public auditability technique for cloud data security is of significant importance so that users can route to an external audit party to check the data integrity of outsourced data when it is needed also with the fair share algorithm we have maintained fair network bandwidth allocation. Thus our technique achieves high security, performance, and also provides less communication and computation overhead.

REFERENCES

[1] H. Shacham, B. Waters,"Compact proofs of retrievability", in Proc. of Asiacrypt 2008, Vol. 5350, Dec 2008, pp. 90–107.
[2] Cloud Security Alliance (2009),"Security guidance for critical areas of focus in cloud computing", [Online] Available: http://www.cloudsecurityalliance.org
[3] IEEE INFOCOM 2010, San Diego, CA, March 2010.
[4] P. Mell, T. Grance (2009),"Draft NIST working definition of cloud computing", [Online]Available: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia,"Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
[6] A. Juels, J. Burton S. Kaliski,"Pors: Proofs of retrievability for large files", in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
[7] G. Ateniese, R. D. Pietro, L. V. Mancini, G. Tsudik, "Scalable and efficient provable data pos-session", in Proc. of SecureComm'08, 2008.
[8] S. Wilson (2008),"Appengine outage", [Online] Available: http://www.cio-weblog.com/50226711/appengine outage.php.

[9] B. Krebs,"Payment Processor Breach May Be Largest Ever", [Online] Available: http://www.voices.washingtonpost.com/ securityfix/2009/01/payment processor breach may b.html, Jan. 2009.
[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song,"Provable data possession at untrusted stores", Cryptology ePrint Archive, Report 2007/202, 2007, [Online] Available: http://www.eprint.iacr.org/.
[11] M. A. Shah, R. Swaminathan, M. Baker,"Privacy-preserving audit and extraction of digital contents", Cryptology ePrint Archive, Report 2008/186, 2008, [Online] Available: http:// www.eprint.iacr.org/

Mrs.V.Kavitha Chandrakanth working as a Senior Assistant Professor, Christ College of Engineering and Technology, affiliated to Pondicherry University, Pondicherry. Completed post graduation M.E (CSE), in Hindustan College of Engineering and Technology, Anna University. Under graduation B.E (CSE), at Mailam
Engineering College, Madras University

Mrs.P.Jamuna pursuing as M.Tech (CSE) - final year, Christ College of Engineering and Technology, affiliated to Pondicherry University, Pondicherry. Under Graduation B.Tech (IT), at Pauls Engineering College affiliated to Anna University, Thindivanam.