**IOSR Journal of Engineering (IOSRJEN)**
**e**-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 5 (May. 2013), ||V3 || PP 01-05

# Enabling Public Auditing for Secured Data Storage in Cloud Computing

[1] Er.Amandeep Kaur, [2] Mr Sukhwinder Singh
Student of Yadvindra College of Engineering Talwandi Sabo, Bathinda,
,Assistant Professor ,Dept. of Computer Science, Yadvindra College of Engineering Talwandi Sabo,Bathinda

***Abstract:*** Cloud computing is an internet based computing which enables sharing of services. Many users place their data in the cloud, so the misuse of data and safeguarding the Cloud Service Provider and Cloud User is a prime concern. This work studies the problem of ensuring Cloud Service Provider and Cloud User both do not take advantage of each other data storage in cloud computing environment. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that cloud users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor to check the integrity of outsourced data and be worry-free. The new auditing scheme effectively does not bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden in terms of computational overhead to cloud user. This new scheme privacy-preserving public auditing process is implemented and performance of such audited with respect to its computation overhead and timing have being analyzed
.

***Keywords:*** Data storage, privacy-preserving, public auditability, cryptographic protocols, cloud computing.

## I. INTRODUCTION

The basic idea of this paper is to motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, and the scheme must enable an external auditor (public) to audit user's outsourced data in the cloud without learning the data contents. The auditing scheme must support scalable and efficient public auditing in the Cloud Computing and the scheme must achieve batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

## II. PROBLEM STATEMENTS

Since the considered a cloud data storage service involving three different entities, as illustrated in Fig. : the cloud user (CU), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by the cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources ; the third party auditor (TPA), who has expertise and capabilities that cloud users do not have to safeguard interest of both the Cloud user and Cloud service provider and is trusted to assess the cloud storage service reliability on behalf of the user upon request. It is considered that the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. It is assumed that the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. However, it harms the user if the TPA could learn the outsourced data after the audit.

## III. METHODOLOGY:

The proposed framework supporting auditing consists of three phases:

a) Public Auditing Service by TPA (Third Party Auditor)
b) Public and Private Keys and Token Generation (key pair)
c) Accessing cloud based resources

In this step all the authentication requirements (key management ) of the three parties are covered before the actual retrieval of data file from cloud based relying party (cloud service provider) and the process of public auditing is implemented.

1. Cloud based Service Provider (Service Provider) public auditing and verification will register itself to third party auditor by giving some credentials and by paying some fees.
2. Third party auditor will issue (Private Key, Public key, key pairs) values to RP (Service Provider)
3. Cloud User will request and some data file (resource) Token Policy from RP (Service Provider).
4. CSP (Cloud Service Provider) will give response to user with (Token Policy, Third party auditor Name isDomain Name URL).
5. Cloud User will request to Third party auditor (TPA) public policy and request for Security Token and send (Resource, Domain Name ) which will make both tracetable and auditable.
6. Now, Third party auditor (TPA) will audit and check the credentials of CSP in its public database, if it exists in database then go to the step of Token Generation; else it will abort the process. Since, the cloud service provider is not publically auditable or tractable.

**4.1 Making Public auditing Services:**

***4.1.1 Token Generation for public auditing:***

This is the step where token is created and send by the TPA to the cloud user and then CSP after encrypting token with the public key of RP (cloud service provider) send to it and after checking (public audit) the access is granted to the cloud user.

1. The TPA will send Audit Security token and public key of CSP (cloud service provider) to cloud user which will be recorded for auditing , traceability and verification.
2. Cloud User will get a encrypted security (attribute-key) token with public key of RP and send it to CSP (cloud service provider) .
3. CSP will decrypt it with its private key and access the credentials of cloud user if they are correct it will give right to access to data file resource.
4. Cloud User can access the resource available on CSP s cloud i.e. can get a file.

**4.1.2 Auditing Scheme:**

To achieve and support privacy – preserving public auditing, we propose to uniquely integrate the homomorphic audit authenticator with random mask technique to trace and audit the process. In our protocol, the sampled blocks files in server's response are masked with the randomness generated by a pseudo random function (PRF). The whole function has done through the TPA functionality.

Let G1, G2 and GT be the multiplicative cyclic groups of prime order p, and e :

G1 x G2 → GT be a bilinear map as introduced in preliminaries. Let g be the generator of G2. H(.) is a secure map –to-point hash function : {0,1}* → G1 , which maps strings uniformly to G1. The proposed scheme is as follows:

***4.1.3 Setup Phase:***

The TPA runs KeyGen to generate the system's public and secret parameters. He chooses a random x, random element u ← G1 and computes v← g x. The secret parameter is sk = (x) and the public parameters are pk = (v, g, u, e (u, v)). Given data file F = (m1, m2, ……, mn) the TPA runs SigGen to compute signature for each block.

***4.1.4 Audit Phase:***

During the auditing process, the TPA picks random element subset I = {s1, ….,sc} of set [1,n] and upon receiving challenge during these process the CSP runs GenProof to generate a response proof of data storage correctness. Specifically, the CSP chooses a random element r ← Zp via r = f (k)prf where (k)prf is the randomly chosen PRF key by CSP for each auditing and calculates R = e(u, v). Meanwhile, the CSP also calculates an aggregated signature σ = Ji ε I σi. It then sends the response proof of storage correctness of the TPA. With the response from the CSP, the TPA runs VerifyProof to validate the response by first Computing γ and then verify the all credentials.

1. Let Tx be the number of resource acessable by CloudUser
   Tx = { Resource1, Resource2, Resource3, ….$Resource_n$}
2. Let Cu be the number of CloudUsers that can access the resource
   Cu = { Cu1, Cu2, …. $Cu_n$}
3. Basic structure of cloud user be represented as
4. CloudUser : Name Email ID Public key Security token
5. Let n be number of requests to the cloud service provider.
6. Let CSP be number of cloud service provider
7. CSP = {CSP1, CSP2, …. $CSP_n$}
8. Basic structure of CSP be represented as

9. CSP: Name ID ResourceID Public key Private key
10. Let n be the number, Let TPA be the external Third Party Auditor represented by variable.
11. TPA: Name Issue Issue Issue Register Register Verify

## IV. RESULTS OF THE PROPOSE SCHEME

We were able to demonstrate a auditing schema that motivates the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, The proposed schemed here enabled an external auditor to audit user's outsourced data in the cloud without learning the data contents and also by safeguarding the identity of cloud user and make trustworthy to interact with Cloud service provider which can be seen from the following results .Then the System we have build supports scalable and efficient public auditing in the Cloud Computing as any number of cloud users and CSP can work together .The objective of privacy-preserving ensuring that the TPA cannot derive users' data content from the information collected during the auditing process has also been implemented. The storage correctness was also ensured in which there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact. Now, let's check the performance of the audit processes. .

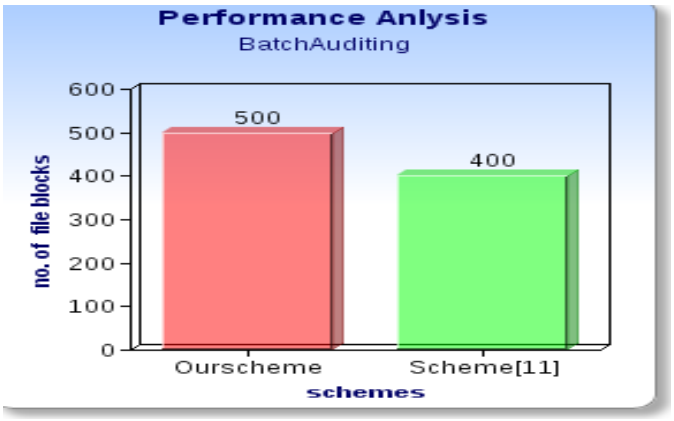


**Fig 1 : No. of Blocks Vs Schemes**

It can be seen from the Fig: that the number of file blocks which have been used in our auditing scheme over more than 20% as compared to the last proposed scheme. Therefore, we can conclude that the new proposed scheme is taking more blocks as compared to last proposed scheme which is highly beneficial and interactive for batch auditing process. As the number of file blocks is higher as compared to last proposed scheme then the proficiency of batch auditing is very high.

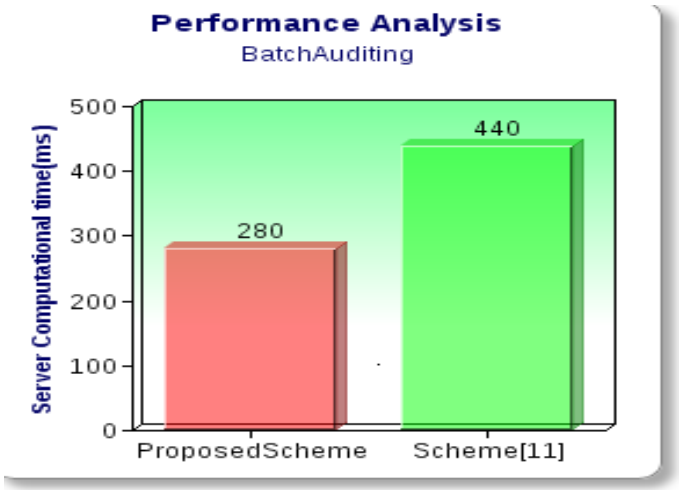


**Fig 2 Server Computational Time Vs Schemes**

It can be illustrated from the Fig 2 that the computational time taken by batch auditing in proposed scheme is only 280ms as compared to 440ms as the basic scheme. This may be attributed because the experimental set up which we are using is on a better hardware platform & it may also be attributed to the fact that which we are using Cloudsim for multithreading process.

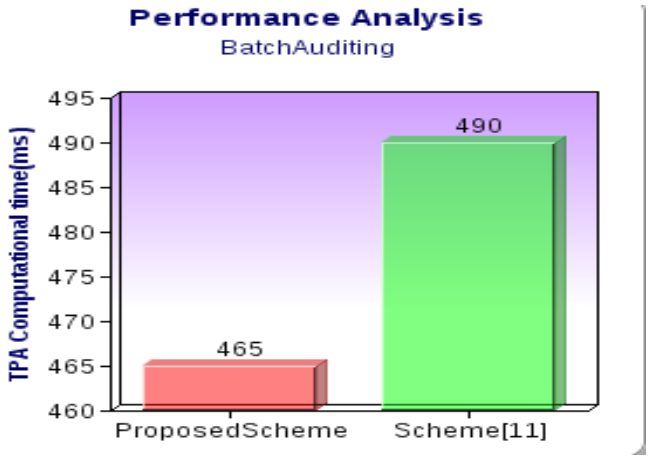


Fig 3 TPA computational time Vs Scheme

It can also be illustrated from the Fig that the TPA computational time taken by batch auditing in proposed scheme is only 465ms as compared to 490ms as the basic scheme. This may be attributed because the experimental set up which we are using is on a better hardware platform & it may also be attributed to the fact that which we are using Cloudsim for multithreading process.So, less time taken by the proposed scheme as compared to the last scheme for auditing process.

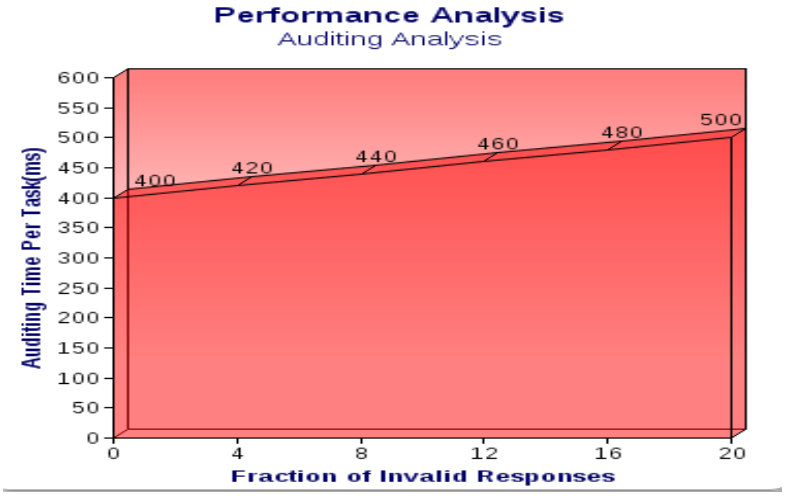


**Fig 4** Auditing time per task Vs Fraction of invalid response

It can be seen from the Fig that as the Auditing Time Per Task increases then Fraction Of Invalid Response certainly increases which idicates higher bit rate of performance

.

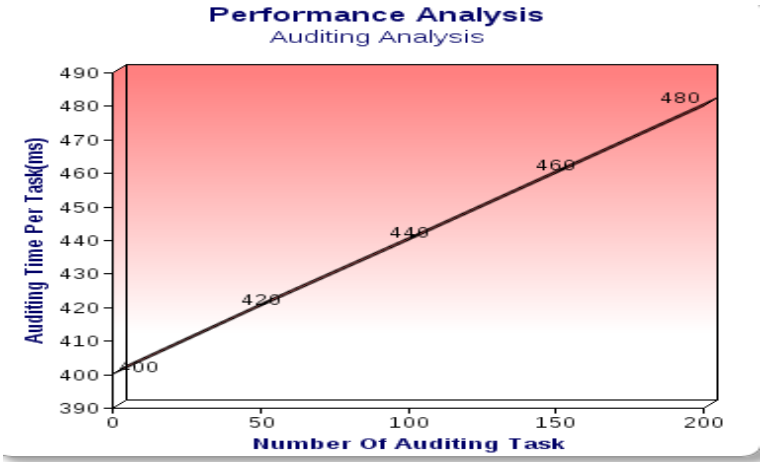


**Fig 5 Auditing Time Per Task Vs Number Of Auditing Task**

It can also be obtained from the Fig 5.5 that as the auditing time per task increases then the number of auditing task simultaneously increses which is highly proficient and valuable for the whole process.

## REFERENCES

[1]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[2]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS.Springer-Verlag, Sep. 2009, pp. 355–370.

[3]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009

[4]. H. Shacham and B.Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[5]. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. Of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[6]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.

[7]. Haley Beard , "Cloud Computing Best Practices for Managing and Measuring Processes for On-demand Computing, Applications and Data Centers in the Cloud With Slas" July 2008 .

[8]. Kerry Brown, Martin Laue, Javier Tafur, Muhammad Nateque Mahmood, Pascal and Keast " An integrated approach to Strategic Asset Management" Third International Engineering Systems Symposium CESUN 2012, Delft University of Technology, 18-20 June 2012.