Privacy-Preserving Public Auditing Using TPA for Secure Cloud Storage

M.Prabha
Student, Department of Computer Science and Engineeering, University College of Engineering Nagercoil

S.Suvetha
Student, Department of Computer Science and Engineeering, University College of Engineering Nagercoil

C.Sangeetha
Student, Department of Computer Science and Engineeering, University College of Engineering Nagercoil

K.L.Neeela
Assistant professor, Department of Computer Science and Engineeering, University College of Engineering Nagercoil

Abstract-Cloud computing is the long unreal vision of computing as a utility and it is also known as on-demand computing. Cloud computing is the dynamic delivery of IT resources like hardware and software and capabilities as a service over the network. However, the actual fact that users not have physical possession of the presumably massive size of outsourced information makes the information integrity protection in Cloud computing a really difficult and probably formidable task, particularly for users with strained computing resources and capabilities. Existing privacy-preserving public auditing protocols assume the tip device of user's square measure powerful enough to cipher all big-ticket operations in real time once the knowledge to be outsourced is given. In fact, the tip devices might also be those with low computation capabilities. so the planned system is employed for 2 light-weight privacy-preserving public auditing protocols.TPA ought to be able to expeditiously audit the cloud information storage without demanding the native copy of knowledge, and introduce no extra on-line burden to the cloud user. The third party auditing method ought to herald no new vulnerabilities towards user information privacy. The algorithmic rule planned here is online/offline algorithmic rule. Thus the proposals support batch auditing and information dynamics.

Index Terms—TPA, batch auditing, data dynamics, privacy-preserving, information integrity

1. INTRODUCTION

Cloud computing could be a promising computing model that allows convenient and on-demand network access to a shared pool of computing resources. Cloud Storage is a very important technique to store the information from the native system to the cloud. And it is an aggregation of computing resources, networking solutions, storage management solutions and virtualization applications which are available on demand, and delivered economically. It is an emerging model through which user gain access to their applications from anywhere at any time through their connected devices. The cloud storage service (CSS) plays a very important role in information storage. As a result of it's chiefly designed, to relieve the burden of storage management and it is managed by the cloud service supplier (CSP) [1]. Cloud service providers also manage an enterprise-class infrastructure that offers a scalable, secure and reliable environment for users, at a much lower marginal cost due to the sharing nature of resources. Despite the fact that it's expeditiously designed it also follows a number of safety risks: First, the cloud computing infrastructures area unit suspected to the interior threats; next, there could also be an opportunity for CSP to behave undependably toward cloud users. Historically, homeowners will check the information integrity by two-party storage auditing protocols. There in user solely allowed verifying the information by causation some challenge to the server. Once verification is done, server can send proof to the consumer.

It's associate degree inefficient technique to conduct auditing by each server and user. As a result of each of these entities might manufacture the inappropriate result. To beat this case, third party auditing is developed [9].The integrity of data in cloud storage, however, is subject to scepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users.

Rest of the paper is organized as follows, Section I contains the introduction, Section II contain the related work, Section III contain the Design objectives, Section IV coming up with proposed system, Section V contain Performance analysis, Section VI concludes the work and followed by references.

2. RELATED WORK

Traditional data integrity checking methods are no longer suitable for the cloud storage environment, since it is impractical for users to download the whole data for integrity checking [7].

Agudo et al. [1] identification of some areas where cryptography can help a rapid adoption of cloud computing. Although secure storage has already captured the attention of many cloud providers, offering a higher level of protection for their customer’s data, that provides more advanced techniques such as searchable encryption and secure outsourced computation and which will become popular in the near future, opening the doors of the Cloud to customers with higher security requirements. But it fails to support the large level system.

Zhangjie et al. [2] here a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services is explained. Specifically, in this proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services.

In addition, attribute-based controlling the system also enables the cloud server to restrict the access to those users with same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfils the required predicate, but has no idea on the exact identity of the user. Finally, it also carries out a simulation to demonstrate the practicability of the proposed 2FA system. But the revocation of the user is difficult. If it's needed to revoke a user in this scheme, it need to rebuild the index and distribute the new secure keys to all the authorized user.

Yiteng et al[7] With a cloud storage, users can store the data files on a remote cloud server with a high quality on-demand cloud service and are able to share their data with other users. Since cloud servers are not usually regarded as fully trusted and the cloud data can be shared amongst users, the integrity checking of the remote files has become an important issue. A number of remote data integrity checking protocols have been proposed in the literature to allow public auditing of cloud data by a third party auditor (TPA). However, user privacy is not taken into account in most of the existing protocols. We believe that preserving the anonymity (i.e., identity privacy) of the data owner is also very important in many applications. But it does not support Integrity check in rank order in the search result, when the cloud server is untrusted.

Cong et al.[7] With a cloud storage, users can store their data files on a remote cloud server with a high quality on-demand cloud service and are able to share their data with other users. Since cloud servers are not usually regarded as fully trusted and the cloud data can be shared amongst users, the integrity checking of the remote files has become an important issue. A number of remote data integrity checking protocols has been proposed in the literature to allow public auditing of cloud data by a third party auditor (TPA).

However, user privacy is not taken into account in most of the existing protocols. It is believed that preserving the anonymity (i.e., identity privacy) of the data owner is also very important in many applications. But when document collection is too large, the collection will be divided into sub-collections and stored in different servers, which makes the ranking process to be delayed.

3. PORPOSED MODELLING

To address these issues, it utilizes the technique of public key based mostly appraiser, that allows TPA to perform the auditing while not strict the native copy of information and therefore drastically reduces the communication and computation overhead as compared to the simple data auditing approaches. By desegregation the homomorphism appraiser with random masking, our protocol guarantees that TPA couldn't learn any information concerning the information content stored within the cloud server throughout the efficient auditing method. The aggregation and computational properties of the appraiser is the additional beneath style for the batch auditing. Specifically,th e contribution during this work are often summarized because the following 3 aspects:

- Ensures the general public auditing system of information storage security in Cloud Computing and supply a privacy-preserving auditing protocol, i.e., the theme supports an external auditor to audit user’s outsourced knowledge within the cloud while not learning information on the information content.
- To the simplest of user’s information, this theme is that the prior to support ascendible and efficient public auditing within the Cloud Computing. Particularly, this projected work achieves batch auditing where multiple delegated auditing tasks from whole totally different users are usually performed at identical time by the TPA.

- Proves the protection and justify the performance of the projected schemes through concrete experiments and comparisons with the progressive.

The overall representation of system architecture is represented in figure 1. Three totally different network entities are often identified as follows

1)User: An entity, World Health Organization has knowledge to be hold on within the cloud and depends on the cloud for knowledge storage and computation, are often either enterprise or individual customers.

2) Cloud Server (CS): Cloud servers can be configured to provide levels of performance, security and control similar to those of a dedicated server. But instead of being hosted on physical hardware that's solely used by user, it resides in a shared "virtualized" environment that's managed by the cloud hosting provider. And, payment is only for the exact amount of server space used. Cloud servers also allow you to scale resources up or down, depending on demand, so that you're not paying for idle infrastructure costs when demand is low.

3) Third Party Auditor (TPA): An effective entity which checks the data integrity which is based on the user's request. This reduces the computation cost of the data owner. In cloud knowledge storage, a user stores their knowledge through a CSP into a collection of cloud servers, that square measure running in a very coincident, cooperated and distributed manner. Thereafter, for application functions, the user interacts with the cloud servers via CSP to access or retrieve their information. And then on verifying the user CSP sends verification request to the TPA. Once the TPA receives the verification request of the user, it responds to the CSP as a verification response by substantiate user's details. Mean whereas CSP sends the requested user detail to the information owner then the CSP sends the encrypted file to the requested user provided that the TPA responds with a positive response. So as to decipher the encrypted file knowledge owner requests the TPA to get the random key and send it to knowledge user, therefore the file is decrypted safely with none intervention of any threat.

Thus the projected system is employed for 2 light-weight privacy- preserving public auditing protocols.

a) TPA ought to be able to expeditiously audit the cloud knowledge storage while not strict the native copy of information, and introduce no further on-line burden to the cloud user;

b) The third party auditing method ought to usher in no new vulnerabilities towards user knowledge privacy. The rule projected here is online/offline rule

c) Thus the proposals support batch auditing and knowledge dynamics.

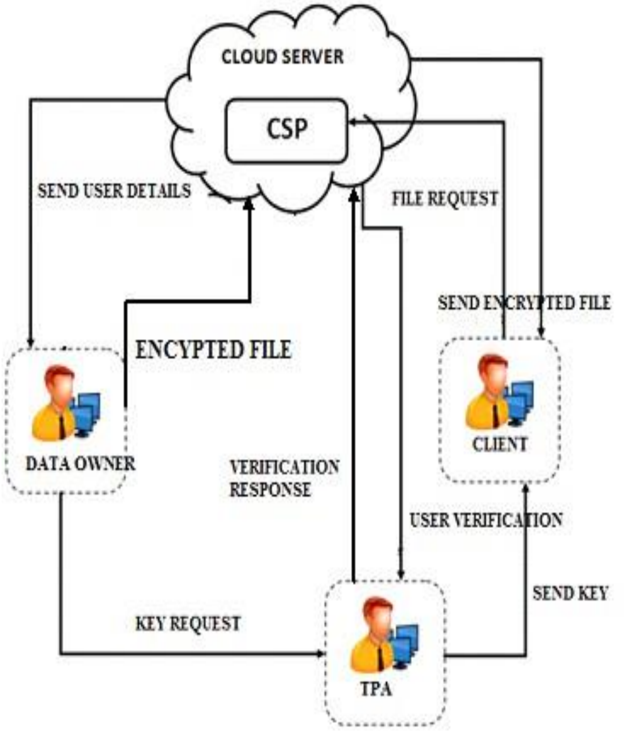

Figure 1 System Architecture

4. PERFORMANCE EVALUATION

Performance evaluation of systems, in general performance evaluation applies to any kind of system like any system which can be build and can measure performance and see whether one is better than the other.

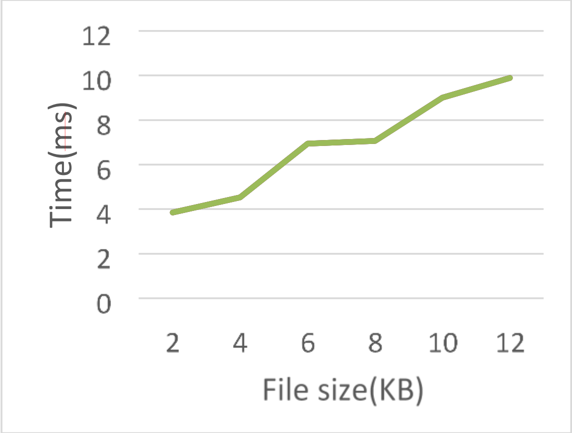

Figure 2 File Size Vs Upload Time

Evaluation of the performance is analyzed for the data in the table 1 and given as a graphical representation in figure 2.This figure explains the performance by taking Time for uploading files and the size of the files as a parameters. And this evaluation is made by keeping the net capacity as 3G network.

File size(KB)	Proposed system
2	3.652266026
4	4.02623105
6	6.339419842
8	6.86339187
10	8.699497938
12	8.889508009

Table 1 File Size Vs Upload Time

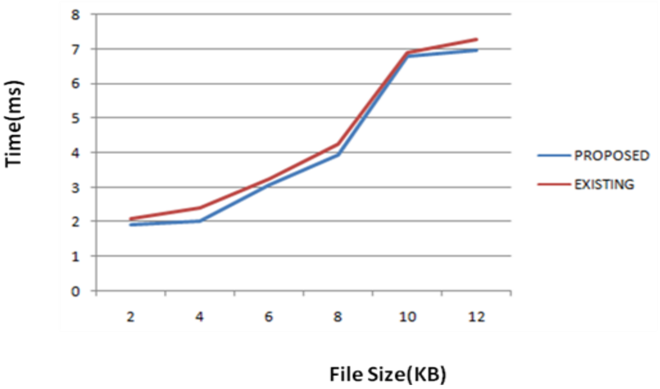

Figure 3 File Size Vs Encryption Time

File Size(KB)	Proposed sytem	Existing system
2	2.10976687	2.509458214
4	2.524684874	2.924684572
6	3.459989874	3.959236893
8	4.248225975	4.648478512
10	7.204389954	7.904857125
12	7.88334897	8.284125885

Table 2 File Size Vs Encryption

In figure 3 performance evaluation between the file size and the Encryption time for the data in table 2 is analyzed. And here Access time of the file and size of the file is taken as a parameters to show the analyze result. And the figure 3 shows that the performance is better in proposed system when compared to that of the existing system. In existing system data are encrypted using RSA algorithm and in the proposed system data are encrypted using Rc5 algorithm. Both these algorithm takes various time to encrypt data. Proposed algorithm is better than the existing algorithm for the encryption technique.

5. CONCLUSION

A privacy-preserving public auditing system for data storage security in Cloud Computing has been proposed. It utilize the random key generation to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files. It further extend the privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e. simultaneously. Extensive analysis shows that the proposed schemes are provably secure and highly efficient.

REFERENCES

[1] Agudo, D. Nu˜ nez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis,"Cryptography goes to the cloud," in Secure and Trust Computing, Data Management, and Applicat., 2011, pp. 190–197.

[2] Zhangjie Fu, Kui Ren, Jiangang Shu "Enabling Personalized Search over Encrypted Outsourced Data " 1045-9219(2015)

[3] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., doi. 10.1109/TPDS. 2015.2506573.

[4] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained twofactor access control for web-Based cloud computing services," IEEE Trans. Inf. Forens. Security, vol. 11, no. 3, pp. 484–497, 2016

[5] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans.Commun., vol. E98-B, no. 1, pp.190-200, 2015.

[6] Y. Feng, Y. Mu, G. Yang, and J. K. Liu, "A new public remote integrity checking scheme with user privacy," in proc. 20th Australasian Conf. Inform. Security and Privacy (ACISP), 2015, pp. 377–394

[7] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, Senior Member, and Wenjing Lou" Public Auditing for Secure Cloud Storage" 0018-9340 (2013)

[8] Lei Zhang, Member, IEEE, Chuanyan Hu, Qianhong Wu, Member, IEEE, JosepDomingo-Ferrer, Fellow, IEEE, and Bo Qin" Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response "(2015)

[9] Mazhar Ali, Member, IEEE, Saif U. R. Malik, Member, IEEE, Samee U. Khan, Senior Member, IEEE" Data Security for Cloud Environment with Semi-Trusted Third Party "(2015)

[10] Emre Yilmaz, Hakan Ferhatosmanoglu, Erman Ayday, and Remzi Can Aksoy" Privacy-Preserving Aggregate Queries for Optimal LocationSelection"(2017)

[11] International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org Volume 3, Issue 3, March 2014 ISSN 2319 - 4847 Volume 3, Issue 3, March 2014 Page 496