Nehru E- Journal
A Journal of Nehru Arts and Science College (Autonomous)
Journal Home Page: http://nehrucolleges.net/jo.html
ISSN: 2349-9052

Research Article
Vol 5 issue 1(2017)
(Jan - July 2017)

AN ANALYSIS AND DISCUSSION OF ISSUES OCCURS IN CLOUD STORAGE SERVICES AND VARIOUS PUBLIC AUDITING MECHANSIMS

A. Kalaivani, Asst. Prof., Dept. of IT,
Nehru Arts and Science College, Coimbatore 641 105, India

Keywords:

Cloud storage, Auditing, Data integrity, third party auditor

Abstract

Cloud computing is most popular in various fields in real world by providing various services and applications to the cloud users as per their requirements. There are many services are provided by the cloud service providers such as IaaS, SaaS, PaaS. Among these cloud storage is the most popular service which is most frequently utilized by the industry peoples to store their large volume of data. As the increased popularity of cloud storages services, issues and threats have also increased simultaneously that attempts to violate security that are provided to the cloud users by corrupting the data's stored in cloud storage. Another problem that might arise in the cloud storage is that data integrity preservation where the industry people would share their data with multiple users who are located in multiple locations. In that case, preserving originality and latest version of data would be a most difficult process where the data's are accessed and modified by multiple users in the distributed manner. This analysis work provides discussion over the various issues that might occur in cloud storage services and remedial techniques which was proposed earlier by various authors. The merits and demerits of earlier methods have been compared to each other in terms of different performance measures. Finally, the evaluations of the works are conducted to find the better technique from which the further proceedings can be carried over in future.

I. INTRODUCTION

Cloud computing is the most popular field which is utilized by various peoples and industry environments an pay per use manner [1]. Cloud computing environment is increasingly becoming popular by providing various services to the cloud users in the optimal manner as per their requirements. Due to the increased popularity of cloud service providers, their incoming has also increased simultaneously which attracts various peoples to invest their amount to start to cloud service provisioning business. Thus the number of cloud service providers has increased in number in the real world, who attempts to handle many marketing strategies to increase their revenue and win other competitors. In that case, quality of cloud services would be degraded by providing the low quality services to the cloud users with reduced time and cost to attract the cloud users from other cloud service providers. This act of cloud service provider would lead to failure which should be tolerated for avoiding the invalid cloud service providers and assuring the secured environment for the cloud users.

Cloud storage is the most popular service which is provisioned by the cloud service providers which enables cloud users to store their

data and contents. Cloud storage eliminates the burden and cost of cloud users from buying and maintaining the cloud storage to store their large volume of data. Cloud storage can be bought as per the cloud user requirements and it can be scaled down or scaled up based on their requests dynamically. As the increased popularity of cloud storage services, cloud user's attempts to store their sensitive data's into the cloud storage, where security becomes the biggest issue. The security of cloud users need to be preserved by preventing data from corruption. And the data integrity needs to be maintained for the better maintenance and provisioning of the latest edited versions to the cloud users who attempts to access the data contents. Thus the main issues that might arise in the cloud storage are given as follows:

- ✓ Data Corruption
- ✓ Data Stealing
- ✓ Data Integrity

From the issues mentioned above, data integrity becomes the biggest issue in the real world environment which needs to be preserved well for the better maintenance of the data and assuring the users from obtaining updated data contents. However data integrity becomes the most challenging task to maintain due to distributed nature of the data contents. Most of the real world applications require the fresh and updated copy of contents to be delivered which will be a more challenging task in the third party server. There are research methodologies has been proposed earlier which focus on ensuring the improved handling of the public auditing tasks and is discussed in the detailed manner in the proceeding sections. The public auditing is performed in various ways by different authors that are going to be discussed in the proceeding sections.

The main contribution of this research work is to analyse the various public auditing protocols and their working procedures along with their merits and demerits. This analysis work provides clear overview of the different methodologies that has been proposed earlier in terms of achieving the secured public auditing process that can lead to obtain the fresh copy of data contents and also prevent the data contents from corruption. The evaluation of the research methodologies has been done in terms of different performance measure to find out the different techniques and their contribution details.

The organization of the research work is given as follows: In this section a detailed introduction about cloud computing and public auditing mechanism has been given. In section 2, entities involved in the public auditing mechanism have been given. In the section 3, different earlier methodologies that has been implemented to process the secured public auditing has been given. In section 4, a comparison of merits and demerits of the methodologies is given.. In section 5, evaluation of those methodologies is done in terms of different performance measures. In section 6, final conclusion of the overall analysis work is given with the better mechanism that can be considered for future research work.

II. ROLES INVOLVED IN THE PUBLIC AUDITING PROCESS

Cloud storage is the most popular service provided by various cloud service providers due to their increased usage by the cloud users and profit. Various roles in the cloud storage service provisioning process that are having main role in causing the effects on public auditing task. Those roles are given along with their responsibility and diagrammatic representation of public auditing process is given in the figure 1.

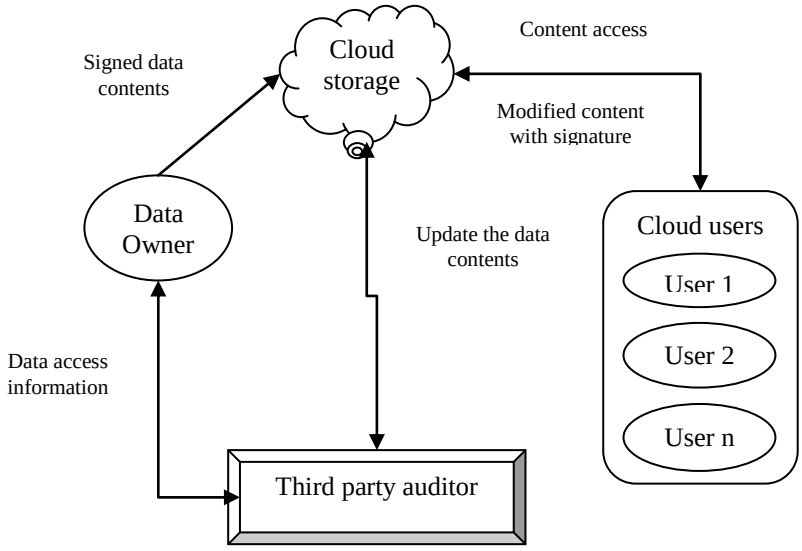

Figure 1. Entities involved in public auditing task

Figure 1 depicts the cloud entities that are involved in public auditing tasks. Various entities that are involved in the public auditing task is described as follows:

Data Owner: Data owner is the one who is original proprietor of data contents. Data owner will encrypt the data contents and will put his signature over the encrypted data. This encrypted and signed data would be stored in the cloud storage.

Cloud Users: Cloud users would access the data contents that are stored in the cloud storage by the data owners. Cloud users would be permitted to access the data contents only if they are genuine and have valid access permission keys.

Cloud Server: Cloud server is maintaining the storage space in which data contents would be stored which are sent by the data owners. Cloud server will check the identity details of the cloud users before providing the data contents to the cloud users. And also, it allows third party servers to perform public auditing on the cloud stored contents.

Third party server: TPA is responsible for performing audit checking on the cloud stored contents. TPA would update the contents stored in the cloud server if they are modified or deleted by the cloud users.

III. OVERVIEW OF EARILER RESEARCH METHODOLOGIES

This section provides a detailed overview of the different methodologies that have been conducted to perform the public auditing in the secured manner. There are lots of methods implemented by various authors and they concluded their methodologies with merits and demerits. Some of the research works that has been conducted previously are discussed as follows:

D. Srinivas et al [2] introduced a secured cloud storage system that can perform auditing with the concern of privacy policy of users. This work reduces the burden of cloud storage providers by outsourcing the auditing process to the third party servers. The third party auditor (TPA) can perform public auditing in the efficient manner with the concern of the data user privacy and preventing them from the additional burdens. Homomorphic non- linear authenticator and random masking mechanism is utilized in

this work to prevent the TPA from learning sensitive information of cloud service providers. This mechanism can also prevent the cloud third party servers and cloud storage servers from stealing of data's that are stored in the cloud storage. The performance evaluation of this work proves that, burden of users can be reduced in a considerable manner along with the satisfaction of the privacy policy of users.

The above research work might cause from the data modification attacks and server colluding attacks which degrades the system performance with reduced security level.

Miss. Nupoor M et al [3] introduced a novel mechanism to perform public auditing which is done by using the third party auditor. The RC5 algorithm is used in this work for preventing the TPA from accessing the sensitive information users effectively. Various cloud storage mechanisms leads to the security violation by corrupting the data contents that are stored in different servers in the distributed manner. An RC5 algorithm ensures the improved security in the distributed environment by generating the random keys in every iteration. This algorithm can provide the secured environment for the cloud users by assuring the prevention of data modification techniques along with the server colluding problems. The performance evaluation proves that this approach overcomes the issues occurring in the previously defined methodology and provides more security.

However this research work cannot ensure the freshness of guaranteed data freshness in the distributed environment which might lead to delivering the un updated version of data contents to the cloud users.

P. Maheswari et al [4] introduced the authentication file system which attempts to preserve the data integrity in the secured manner with the help of third party auditor. This method ensures 100 % guaranteed data freshness preserves by generating the distributed environment that can periodically check the freshness of the content. Along with the data freshness, this method also provides the assured data privacy, so that the secured environment can be guaranteed for the cloud users. These goals are achieved by introducing the new ring signature scheme through which one can update the contents that are residing in the cloud server in the distributed manner. This mechanism would allow users to update the contents only if they pose the ring key at the time of updation. Else they would be prevented from modifying or accessing the contents that are stored in the cloud environment.

All the research work mentioned above having computation burden problem due to the nature of third party auditor who will request the locally stored data content copies to preserve the data freshness.

S.Ezhil Arasu et al [5] proposed a novel framework for public auditing which make use of HMAC algorithm to ensure the data integrity along with the data privacy. This algorithm doesn't require locally stored data files for performing the public auditing process. It can check the data freshness periodically in run time with the help of last retrieved data contents from the cloud servers. This mechanism leads to the efficient handling of the data contents with improved security by encrypting the cloud stored content using the HMAC algorithm. The decoding of the secret information that are generated using HMAC algorithm would be a more difficult process due to random generation of long bit length of keys. The performance evaluation of this work ensures the guaranteed system performance without degradation.

The above mentioned research works are based on complete auditing which requires retrieving the entire contents that are stored in the cloud server. This nature might lead to the missing version updation and also more computation overhead.

T. Prasanthi et al [6] introduced the secured public auditing mechanism which overcomes the issues that occurred in the previously mentioned research works by introducing the novel concept called the batch auditing tasks. This batch auditing task eliminated the computation overhead by avoiding the necessity of downloading the entire contents from the cloud server for version updation. Instead of that, batch auditing leads to retrieval of contents which is only required to be updated. This method reduces the computation overhead in the considerable manner than other methodologies by eliminating the need of downloading the entire contents from the network. This method will divide the data contents into multiple partitions before storing it in the cloud server. Thus only the required part can be downloaded for the performing public auditing.

Permission for Simultaneous access the cloud users is prohibited in all of the research works that are discussed previously. Anyone of the user only can access the data contents and other should wait in queue until others finish their tasks.

Jyoti R Bolannavar et al [7] introduced the novel mechanism to perform secured public auditing that can enable multiple users to access and modify the particular data contents simultaneously. This work also ensures the better data integrity level than the other methodologies. This is achieved by introducing the Privacy-Preserving Public Auditing Scheme that can access the data contents which are stored in the cloud storage in an efficient manner. This will provide the multiple tokens to the multiple users who want to access and modify the contents at the same time. The TPA will monitor and record the changes that are done by every user who hold valid tokens in their hand and those changes would be reflected in the local distributed copy of those corresponding files. The evaluation of this methodology proves to provide better data freshness assurance than other methodologies.

Previously defined mechanism has more computational complexity which needs to be resolved effectively to provide improved handling and performance of public auditing with assured data freshness.

Boyang Wang et al [8] introduced the novel mechanism namely oruta which will adapts the signature generation algorithm to keep track of modification performed by the multiple cloud users simultaneously. This approach allows users to perform modification on the data contents only if they pose valid access permission keys. After performing modification, user will generate their signature over the modified contents which will make ease of public auditors. With the help of the newly generated signature, public auditor can easily find that the some modification is done in the corresponding data files. This leads to the efficient handling of data contents and data integrity is maintained with reduced computation complexity than the previous research works.

The previous research work cannot assure the legal trust for the cloud stored contents, thus the data owners would resist storing their contents in the cloud storage which would degrade the system performance.

Hui Tian et al [9] proposed a novel mechanism namely Dynamic Hash Table mechanism which increases the legal trust level of the cloud data owners. This mechanism implements the two dimensional data matrix in which identity information and the public auditing information would be stored by the third party service providers. This work transfer the authorization permission from the cloud service providers to the third party auditors, thus the security level of the cloud service providers will get increased. The structural representation of the DHT leads to the efficient and flexible updation of the data contents that are retrieved by the cloud data owners. The performance evaluation of the proposed methodologies leads to the efficient handling and assurance of data integrity with the help of BLS signature concept.

All the research methodologies discussed above attempts to perform public auditing an efficient manner with the concern of privacy level of users data files. All these mechanism having both merits and demerits are discussed in the detailed manner and lists out the information in the following sections.

IV. COMPARISON OF DIFFERENT METHODOLOGIES

This section provides the detailed overview of the different methodologies along with their name. The benefits and issues that are occurring each methodology are given in the tabular format. The following table 1 lists out the names of the methodology and merits and demerits of those corresponding methodologies.

Table 1. Comparison of various research methodologies in terms of their merits and demerits

S.No	Title	Author	Method	Merits	Demerits
1	Privacy-Preserving Public Auditing In Cloud Storage Security	D. Srinivas	Homomorphic non- linear authenticator and random masking	Improved data privacy protection Reduced burden of users More security	Any possible leakage of user sensitive data can lead to the violation of effective maintenance of tasks
2	Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm	Miss. Nupoor M. Yawale, Prof. V. B. Gadichha	RC5 algorithm	Prevention from data modification techniques Can avoid the causes that might occur due to cloud server colluding problems	User files are encrypted by different authorities It doesn't concentrate on privacy conditions of the cloud users
3	AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud	P. Maheswari, B. Sindhumathi	new ring signature scheme	Assured handling of data contents with guaranteed data freshness level Can provide secured environment in the distributed cloud environment	Offline accessing of information cannot be handled well The data freshness might get violated in the offline mode of network
4	Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm	S.Ezhil Arasu, B.Gowri, S.Ananthi	HMAC Algorithm	Improved handling of data contents More privacy with assured data freshness	Many attempts might lead to corruption of data contents that are stored in the cloud environment More complex to implement due to its complex working procedure
5	An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing	T. Prasanthi, C. Balasubramanian, S. Kimsukha Selvi, K. Kala	Batch Auditing task	Reduced computation overhead Resource wastage can be avoided considerably such as bandwidth, memory and so on Provide more flexible environment for the cloud users	It cannot perform well in the distributed environment due to multi entities who can access contents simultaneously
6	Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage	Jyoti R Bolannavar	secure cloud storage system	Enable simultaneous accessing of data contents Improved handling of the multi user updated contents	More complex to handle this distributed nature Monitoring and keep track of all the cloud stored contents might lead to the missing and corruption of data contents
7	Oruta : Privacy-Preserving Public Auditing for Shared Data in the Cloud	Boyang Wang, Baochun Li, and Hui Li	Oruta	Reduced computation overhead Can preserve the data integrity with improved security and privacy of users	There might be an chance of incorrect audit proof occurrence in the cloud environment These incorrect audit might reduce the efficiency of the batch auditing tasks

8	Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE Transactions on service computing	Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen, Jin Liu	secure cloud storage based on dynamic hash table (DHT)	Improved trust level of cloud users Less computation overhead by avoiding the vulnerable entities Public auditing is performed in the genuine manner which can lead to the convenient environment for the cloud users	Verification overhead of third party auditor is more due to handling of both authentication and public auditing mechanism Multiple audit requests from different users would be more difficult to handle

V. COMPARISON OF PREVIOUS METHODOLOGIES BASED ON AUDITING TIME

Various research works have been introduced earlier that focus on performing the public auditing in secured and privacy concern. Some of the previous methodologies have been discussed in depth in the previous section to find the merits and demerits of all the methodologies. The performance measure that can be used to measure the performance improvement of each methodology and their auditing time. The performance comparison is given in detail in the following sub section.

Auditing time is a total time taken to perform auditing task from the time of data content that are retrieved to the time when it uploaded again after updation. The auditing time of the effective method should be less than the other methodologies which is evaluated in the following sections. The graphical representation is given as like as follows:

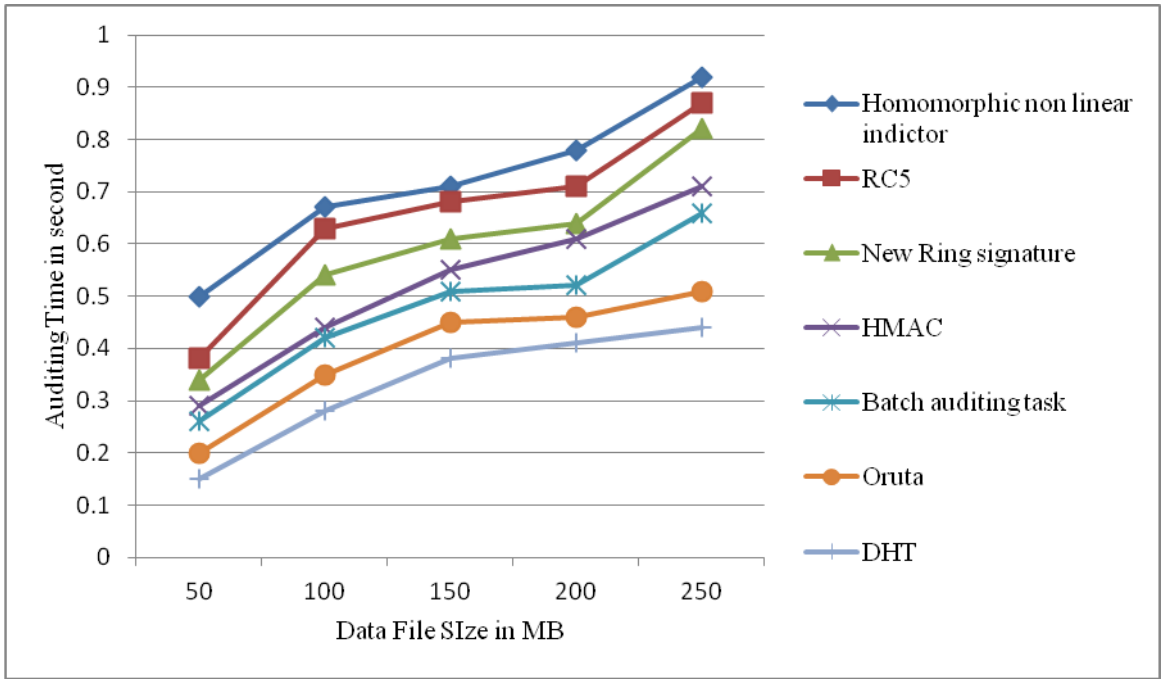

Figure 2. Auditing Time comparison

The figure 2 depicts the comparison analysis of auditing time consumed by different methodologies in terms of varying data file sizes. From this analysis it can be proved that the dynamic hash table based public auditing mechanism can perform better public auditing than the other methodologies in terms of different file sizes.

VI. CONCLUSION

Public auditing is the most important task in cloud computing environment which needs to done with more concern to assure the delivery contents with improved data freshness. In this research analysis, various research methodologies proposed earlier by different authors have been discussed in detailed to find the merits and demerits of them. The evaluation of this research methodologies leads to the finding of better approach that can be proceeded to find the future research works to guarantee a secured environment in the real world application. The final evaluation of this work concludes that the benefits of all the methodologies can be combined together to generate the novel approach by using which real world application can be handled efficiently.

REFERENCE

[1] P. M. Mell and T. Grance, \The nist definition of cloud computing," Technical Report: SP 800-145, 2011.

[2] D. Srinivas, “Privacy-Preserving Public Auditing In Cloud Storage Security”, International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2691-2693

[3] Miss. Nupoor M. Yawale, Prof. V. B. Gadichha, “Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[4] P. Maheswari, B. Sindhumathi, “AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud”, IOSR Journal of Computer Engineering (IOSR-JCE), PP 56-63, 2013

[5] S.Ezhil Arasu, B.Gowri, S.Ananthi, “Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013

[6] T. Prasanthi, C. Balasubramanian, S. Kimsukha Selvi, K. Kala, “An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing”, Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K.

[7] Jyoti R Bolannavar, “Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage”, International Journal of Scientific Engineering and Research (IJSER), Volume 2 Issue 6, June 2014

[8] Boyang Wang, Baochun Li, and Hui Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE transaction on Cloud computing, Volume:2 , Issue: 1, 2014

[9] Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen, Jin Liu, “Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage”, IEEE Transactions on service computing, Volume:PP , Issue: 99, 2015