ADVANCED MECHANISM OF INTELLIGENT THIRD PARTY AUDITOR IN CLOUD COMPUTING

Monisha Chauhan[*]

Dr. Mamta Bansal*

Dr. R.P. Agarawal*

ABSTRACT-

Cloud computing has been used for data storage as well as computational purposes. It is internet based computing through which we share data along with various services also. The main and important concerns about the cloud storage services are authorization and trust management for the cloud service provider(CSP).Third Party Auditor(TPA) plays important role to achieve these problem.TPA has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage security. In this paper we give and discuss about few emerging trends in cloud computing as well as we proposed a new model i.e. Intelligent Third Party Auditor(ITPA).This model used various technique like compression, encryption ,Meta data with all related operation(Insertion, Deletion, Update) .This proposed model are introduced for confidentiality, integrity and access control for cloud storage systems.

Keywords-Cloud Computing, Third Party Auditor(TPA),Cloud Security, Cloud Service Provider, Encryption Technique, Compression Scheme.

[*] Shobhit University, Meerut

1.INTRODUCTION

Many technologies are coming in the Cloud Computing, which provides Internet-based service and use of computer technology. This is cheaper and more strong processors, together with the software as a service (SaaS) computing architecture, are transforming data into data centers on huge scale. The increasing network and flexible network connections make it even possible that users can now use high quality services from data and provides remote on data centers.

Cloud Computing is a model that provides on demand services to the users in convenient and efficient manner. This model contains a shared pool of resources like networks, servers, storage, Applications and services.

Types of Cloud Services:

Software as a Service (SaaS) In this Service Users are provided access to software applications and Databases. This is also called as On Demand Software services. The cloud user need to pay to use the cloud software applications. Infrastructure as a Service (IaaS) the Cloud Service provider supply the resources on demand basis from their Data centers. The resources are Software bundles, Raw, Virtual local area networks, load balancers, firewalls, IP addresses, Virtual machine disk image library, file based storages. Platform as a Services (PaaS) the Cloud Service provider a computing platform to the program developers. Computing platform includes operating system, programming language execution environment, database, and web server.

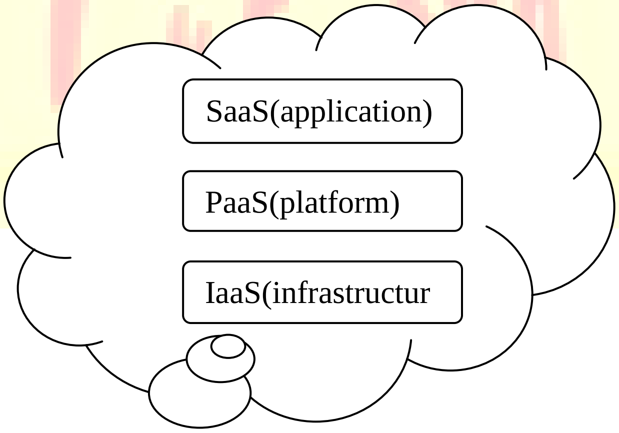

Fig. 1.1 Cloud Architecture

Benefits of Cloud Computing:-

1. Achieve economies of scale
2. Reduce spending on technology infrastructure. Globalize your workforce on the cheap.
3. Streamline processes.
4. Reduce capital costs.
5. Improve accessibility.
6. Monitor projects more effectively.
7. Less personnel training is needed.
8. Minimize licensing new software.
9. Improve flexibility.

Cloud computing provide us high-performance computing and storage infrastructure through web services. Highly secure data storage must be needed in this architecture. Increasing the adoption of cloud storage services, we have to make highly secure cloud storage system which has the aim to achieve the best of both world by providing the security of a private cloud and the functionality and cost saving of a public cloud. In any type of cloud we have to protect the cloud storage by getting different security techniques. Any secure cloud storage system must have the following security services:-

1.Confidentially

2.Integrity

3.Availability

4.Reliability

5.Efficient retrieval.

6.Data Sharing

2. EMERGING TRENDS IN CLOUD COMPUTING

The global IT scenario with its array of products, solutions and services is changing. New challenges are emerging with the fast advent of technology. These emerging changes and trends have given us an opportunity to redefine ourselves and focus our vision towards unparalleled innovation. Source Edge believes that acknowledging and inculcating the latest technology innovations in our services and solutions will provide the significant insight required to stand out of the crowd and fuel our passion to lead the industry.

1) Remote Data Integrity Checking in Cloud Computing[17]

Cloud computing is an internet based computing which enables sharing of services. It is very challenging part to keep safely all required data that are needed in many applications for user in cloud. Storing our data in cloud may not be fully trustworthy. Since client doesn't have copy of all stored data, he has to depend on Cloud Service Provider. This work studies the problem of ensuring the integrity and security of data storage in Cloud Computing. This paper, proposes an effective and flexible Batch Audit scheme with dynamic data support to reduce the computation overheads. To ensure the correctness of users data the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud .They consider symmetric encryption for effective utilization of outsourced cloud data under the model, it achieve the storage security in multi cloud data storage. The new scheme further supports secure and efficient dynamic operations on data blocks, including data insertion, update, delete and replacement. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colliding attacks.

The digital signature works by taking the user data first, then perform a hash function over it using Secure Hash Algorithm (SHA). After that, computes the signature for the generated hash value by encrypting it with the private key. In the other side, the decryption is done by the public key but the result will be a hash value, and the hash value is not reversible to its original data.

There are three procedures in our model to satisfy the integrity concept:
Digital signature part will be done by the user.
The CS verifies over the user data in the cloud to check over the manipulation or intrusions in the cloud data.
The TPA verifies over the cloud server part to check if the cloud server was manipulating in the user data or not.

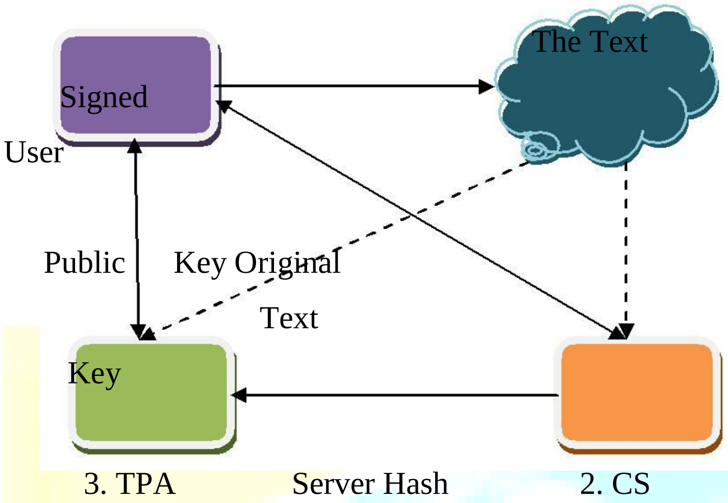

Fig 2.1 : The Proposed Architecture

Future improvement

In this paper , they planned to implement the locking protocol in cloud data storage with the help of CSP for data update. It can give clear security to users own data when users complete his requirement.

2) Secure and Dependable Cloud Services for TPA in Cloud Computing[15]

In this paper, Author's proposed a secure cloud storage system supporting privacy-preserving public auditing. they further extend their result to enable the TPA to perform audits for multiple users simultaneously and efficiently. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks.

Adversary Model

From user's perspective, the adversary model has to capture all kinds of threats towards his cloud data integrity. Because cloud data do not reside at user's local site but at CSP's address domain, these threats can come from two different sources: internal and external attacks. For internal attacks, a CSP can be self-interested, un-trusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on. For external attacks, data integrity threats may come from outsiders who are beyond the control domain of CSP, for example, the economically motivated attackers.

Therefore, they consider the adversary in their model has the following capabilities, which captures both external and internal threats towards the cloud data integrity. Specifically, the adversary is interested in continuously corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data.

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, their aim is to design efficient mechanisms for dynamic data verification and operation .The new design is based on the observation of linear property of the parity vector blinding process. Recall that the reason of blinding process is for protection of the secret matrix P against cloud servers. However, this can be achieved either by blinding the parity vector or by blinding the data vector (we assume k < m).Thus, the overall computation overhead and communication overhead remains roughly the same.

1. Procedure
2. Choose parameters l, n and function f, ø;
3. Choose the number t of tokens;
4. Choose the number r of indices per verification;
5. Generate master key K_{prp} and challenge $k_{chal\,;}$
6. for vector G (j), j ← 1, n do
7. for round i← 1,t do
8. Derive $\acute{\alpha}_{i}=f_{kchal}(i)$ and $k^{(i)}_{prp}$ from $K_{PRP.}$

```
end for
end for
Store $v_i$ s locally
end procedure
```

3) Delegating Auditing Task to TPA for Security in Cloud Computing[16]

This paper proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. Extension is introducing Third Party auditing users can safely delegate the integrity checking tasks to third party auditors. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing.. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users.

In this paper, they investigate the problem of ensuring the security and dependability for cloud data storage under the aforementioned adversary model. In particular, their aim is to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:Storage correctness,Dependability,Fast Localization of data error,Dynamic data support and Lightweight.

Introducing erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. RSA Algorithm which reduces the overhead. Less burden for Clients delegating cloud server auditing task to TPA.

Token Precomputation:

Data storage correctness and data error localization simultaneously, our scheme entirely relies on the precomputed verification tokens. The main idea is as follows: before file distribution the user precomputes meanwhile, as all servers operate over the same subset of the indices, the requested response values for integrity check must also be a valid codeword determined by the secret matrix P.

Algorithm 1

Token Precomputation:

```
Procedure
Choose parameters l, n and function f, ø;
Choose the number t of tokens;
Choose the number r of indices per verification;
Generate master key $K_{prp}$ and challenge $k_{chal}$;
for vector G (j), j ← 1, n do
    for round i← 1,t do
        Derive $ά_i=f_{kchal}(i)$ and $k^{(i)}_{prp}$ from $K_{PRP}$.
    end for
end for
Store $v_i$ s locally
end procedure
```

The element $v_i^{(j)}$ belongs to GF (2^p) with small size, it is the response where the user expect from the server when he challenges in a specified blocks.

The user keeps the token locally or in encrypted form of the pre-computed tokens in the cloud server. But in our case the user stores the tokens locally, to avoid lower bandwidth which occur due to dynamic data operation

The final step before file distribution is to blind each parity block $g_i^{(j)}$ in ($G^{(m+1)}$,…………,$G^{(n)}$) by

$$g_i^{(j)} \leftarrow g_i^{(j)} + f_{kj}(s_{ij}),\ i \in \{1,\ldots\ldots\ldots,l\},$$

where k_j is the secret key for parity vector .This key is used for protection. After blinding the parity information, the user disperses all the encoded vectors $G^{(j)}$ (j €{1,….,n}) across the cloud servers S1,S2,……,Sn

Correctness Verification and Error Localization

Correctness Verification and Error localization is the main idea for eliminating the data errors in the system. In the existing system they do not explicitly consider the error localization, thus they give only binary results. But in this scheme we get find the misbehaving servers by using challenge –response protocol

Specially, the procedure of the i-th challenege-response for a cross-check over the n servers is described as follows :

The user reveals the $ά_i$ as well as the i-th permutation key $k_{prp}^{(i)}$ to each servers.

The server storing vector $G^{(j)}$ aggregates those r rows specified by index $k_{prp}^{(i)}$ into a linear combination

Upon receiving $R_i^{(j)}$ all the servers, the user takes away blind values in $R^{(j)}$ ($j €$ {m+ 1, . . . , n})

Then the user verifies the codeword with the received value which is generated but the secret matrix P.

As the entire server operates over the same subset of indices .So these row specified codeword should be in the encoded file. If the above equation holds the challenge is passed otherwise it indicates that the specified row has an error which is passed to the server that there is a corruption.

Algorithm for Storage Correctness and Error Localization

```
procedure CHALLENGE (i)
    Recompute $\alpha i = fkchal (i)$ and kprp from KPRP
    Send { $\alpha i, k( i )prp$ } to all the cloud server
    Receive from servers:
    $\{Ri( j ) = \Sigma rq=1\ \alpha i * G(j)\ [\varphi (i) (q)] | 1 \le j \le n\}$
    for ($j \leftarrow m + 1, n$) do
        $R( j ) \leftarrow R( j ) - \Sigma rq=1\ fk\ j\ (sIq ,j ) \cdot \alpha i\ ,\ Iq = \varphi kprp(i) (q)$
    end for
    if (( Ri ( 1 ) ,…, Ri ( m ) ) • P = = ( Ri ( m+1 ) , . . ., Ri ( n ) )) then
        Accept and ready for the next challenge.
    else
```

```
        for ( j ← 1, n) do
            if (Ri ( j ) ! = vi( j ) then
                return server j is misbehaving.
            end if
        end for
    end if
end procedure
```

File Retrieval and Error Recovery

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that their verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one.

Future Work:

Future research on improving performance of Byzantine failure, malicious data modification attack, and even server colluding attacks.

4) N^{TH} Third Party Auditing For Data Integrity In Cloud[18]

Security is a major issue in cloud computing environment as the resources are dynamic, virtualized, scalable and elastic in nature. Data Integrity is to ensured. Auditing plays a vital role in providing solution to the data integrity in cloud. Highly distributed and non- transparent nature of cloud increases the complexity of Auditing process. Auditing deals with SLA monitoring and compliance.A third party auditor is essential to perform auditing to ensure data integrity on cloud services. In this paper, a Dynamic Third Party Auditing System is proposed in which a third party entity dynamically provides auditing services on cloud computing environment. TPA makes task of Client by verifying the integrity of data stored in cloud .The Dynamic third party auditing system does auditing using public key based homomorphic authentication .

PROPOSED SYSTEM

TPA is the external entity it supports the data integrity in the cloud. Cloud Service Providers transferring the data to cloud user from cloud server. Now the TPA have to check the integrity of transferred data. The process will be like this, The TPA will collect the receive data and send data to verify. If both data same, then there is no violation in the data integrity. Practically this is not possible for the large data. Also TPA also a external entity again if they give full set of data again data integrity question will rise in TPA end. For the multiple cloud and multiple users they need multiple auditing called batch auditing. they need to implement the new technique with Homomorphic authenticator and the bilinear aggregate signature method.

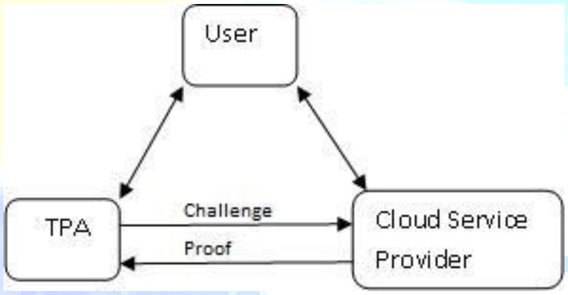

Fig. 2.2 Role of TPA

The TPA process works in three steps: Key Generation , Server integrity proof, integrity verification.

Key Generation: Key generation is done by the Owner. The data is encrypted using the private key of the owner and public key is transferred along with the data.

Server Integrity proof: TPA dispute the server to give a proof of data integrity. The server sends the proof.

Integrity Verification: On receiving the proof from the Server, TPA verifies the integrity without encrypting the data. The tag in the data helps the TPA to check the data efficiently.

The Auditing can be done periodically on samples of data. Over the period, the samples are collected and verification is done for the samples. This type of auditing falls under static category. On verification if the auditor is convinced with the data integrity, the auditor erases the local data

The future work has to be done in concentrating on the scalability of the cloud services Auditing. Scalability is the main characteristics of the cloud. As cloud is highly distributed, the number of distributed nodes in the auditing process is a factor to be considered.

3.PROBLEM IDENTIFICATION

Existing system in Cloud computing providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are just accessing or renting; they can forego capital expenditure and use resources as a service, paying instead for what they use.

Benefits of Cloud Computing:

1. Minimized Capital expenditure
2. Location and Device independence
3. Utilization and efficiency improvement
4. Very high Scalability
5. High Computing power

As they know that the user's data are stored in data centre's , which are remotely located. In this techniques clouds have more security challenges which need to be clearly understood and resolved. One of the major concerns with cloud data storage is that of data integrity verification at un-trusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the advantage of their personal.TPA (Third Party Auditor) have proposed many algorithms as we mentioned in literature survey above. We also agree that it works but still we find lots of problems in security area in cloud computing. In the existing system TPA has the following drawbacks:-

a) TPA demands retrieval of user data, here privacy is not preserved

b) TPA have to remember which key has been used

c) These two schemes good for static data not for dynamic data

Present study suggest to develop new algorithms for removing the security problems which comes in cloud computing like Data centre Security, Network Security, How secure is encryption Scheme etc which depend on the TPA. We will create new algorithm for our secured AMITPA(Advanced Mechanism of Intelligent Third Party Auditor).

4.PROPOSED WORK

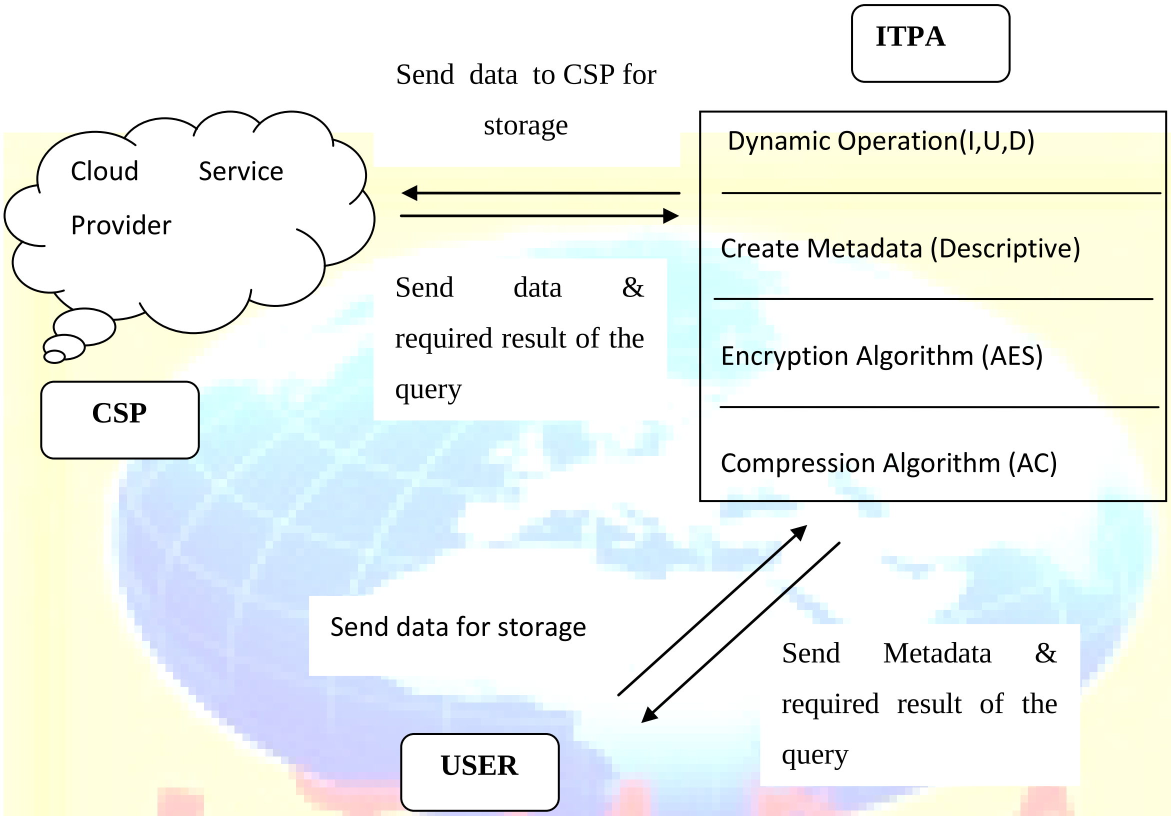
ITPA
Send data to CSP for storage
Cloud Service Provider
Dynamic Operation(I,U,D)
Create Metadata (Descriptive)
Encryption Algorithm (AES)
Compression Algorithm (AC)
Send data & required result of the query
CSP
Send data for storage
Send Metadata & required result of the query
USER

Fig. 4.1 Advanced Mechanism Of Intelligent Third Party Auditor

Cloud computing give us resources in the form of service rather than a product ,utilities are provided to the users over internet. The main goal is to secure ,protect the data and the processes which come under the property of users. It is an special and important research area which requires lots of development from both the academic and research communities. In cloud computing , all resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data.

One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. We proposed secured cloud storage system, by using new security algorithm and maintain the integrity of outsourced data in cloud environment. In the cloud , all data and services are exist in centralized huge data center, which is not easy to handle and not-trustworthy . Our aim is, to design efficient and new mechanism using different techniques with the help of TPA (Third Party Auditor) for data verification and operation and achieve the following goals and also remove the above mentioned drawbacks:-

1. Storage should be correct and kept intact(complete) all the time in the cloud.
2. Data is dynamically available with assurance of data accuracy even if data is modify ,delete or appended by the user in the cloud .
3. Accountability in cloud data - trustable , reliable and customers should be satisfied .
4. Privacy of user data is highly secured.

In the above mechanism of intelligent third party auditor, all file / data should be stored in CSP through ITPA. At the start, files are sending through the ITPA and follows different techniques like Compression, Encryption and creates metadata about the encrypted file and then sent the file to the cloud server for storage. Metadata should be stored on ITPA as well as one copy should also be send to the user for further query, if needed. In this proposed work data is compressed with arithmetic coding technique which is not yet applied before in any model of cloud computing. Data is highly secured in this proposal and kept intact also.

5.CONCLUSIONS

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various schemes are proposed by authors over the years to provide a trusted environment for cloud services. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. This study give us a brief view of different schemes proposed in recent past for cloud data security using third party auditor. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider client. The detailed security and performance analysis shows that the system is highly efficient and flexible to malicious data modification attack and reduce the external threats imposed over the cloud storage with the help of TPA. But we want to resolve all security problems with the help of TPA in highly secured way. So we want to proposed a new mechanism of TPA in cloud computing for ensuring the correctness and integrity of data in cloud storage. We will use compression techniques as well as metadata along with dynamic operation effectively, which makes this system more secure as comparatively other ones.

6. REFERENCES

1.K.Govinda,V.Gurunathaprasad and H.Sathiskumar,"Third Party Auditing For Secure Data Storage in Cloud Through Digital Signature using RSA", *International Journal of Advanced Scientific & Technical Rsearch*, vol. 4, issue 2,Aug 2012.

2.A.Mohta and L.K.Awasthi,"Cloud Data Security While Using Third Party Auditor", *International Journal of Scientific & Engineering Research*, vol 3, issue 6,June 2012.

3.C.Wang, Sherman S.M.Chow, Q.Wang,K.Ren and W.Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", *IEEE Transaction on Computer I*,vol.62,issue 2,Feb 2013.

4. T.Paigude and Prof. T.A.Chavan,"A Survey on Privacy Preserving Public Auditing for Data Storage Security", *International Journal of Computer Trends & Techniques*, vol.4,issue 3,2013.

5. V. Vinaya and P. Sumathi," Implementation of Effective Third Party Auditing for Data Security in Cloud", *International Journal of Advanced Research in Computer Science and Software Engineering*,vol.3, issue 5-May 2013.

6. J.Kaur and J.Singh,"Monitoring Data Integrity while using TPA in Cloud Environment", *International Journal of Advanced in Computer Engineering and Technology*, vol. 2,issue 7,July 2013.

7. Bhagat et al., *International Journal of Advanced Research in Computer Science and Software Engineering* 3(3), Volume 3, Issue 3,March 2013.

8. H.Joshi, Dr. Prof. S.Patil and Prof. M.Pavaskar,"A Survey On Data Security & Accountability In Cloud", *International Journal of Research in Advent Technology* ,vol. 2,issue 1,January 2014.

9. H.T. Dhole, P. C. Papade and Sachin B. Bhosle," Ensuring Data Security using Cloud Computing" , *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, issue 1,January 2014.

10. K.Meenakshi and V.S.George, ”Cloud Server Storage Security Using TPA”. International Journal of Advanced Research in Computer Science & Technology, vol. 2,issue 1-Jan-March 2014.

11. C.Wang ,S.S.M.Chow,Q. Wang,Kui Ren and W.Lou, ”Privacy Preserving Public Auditing for Secure Cloud Storage”, *IEEE*, vol. 62, issue. 2,February 2013.

12.Jain,M.Kumar and A.Lambha,”An Overview and Trends in Cloud Computing”,*International Journal of Computer Application.*

13.B.L.Sahu and R.Tiwari,”A Comprehensive Study on Cloud Computing”,*International Journal of Advanced Research in Computer Science and Software Engineering*,vol. 2,Issue 9,Sept 2012.

14.E.O.Y.Boateng and K.A.Essandoh.”Cloud Computing:The Level of Awareness amongst Small & Medium-sized Enterprises(SMEs)in Developing Economies”,*Journal of Emerging Trends in Computing and Information Science*,vol.4,no. 11 Nov-2013

15.B.B.Nandeesh,G.Kumar and J.Mungara,”Secure and Dependable Cloud Services for TPA in Cloud Computing”, *International Journal of Innovative Technology Engineering*, vol.1,issue 3,Aug 2012.

16.N.Gowri and D.Srinivas,”Delegating Auditing Task to TPA for Security in Cloud Computing”,*International Journal of Research in Computer and Communication Technology*,vol 2,issue 11,Nov 2013.

17. M.V.Khaba and M.Santhanalakshmi,”Remote Data Integrity Checking in Cloud Computing”, *International Journal of Recent and Innovation Trends in Computing and Communication*,vol 1,issue 6.

18.R.K.Ramesh,P.V.Kumar and R.Jegadeesan,”Nth Third Party Auditing for Data Integrity in Cloud”,*Asia Pacific Journal Research*,vol 1,issue 13,Jan 2014.