Cloud Server Storage Security Using TPA

Mr.B.S. Yelure
GCE, Karad
Karad, India
bhushanyelure2008@gmail.com

Mr.Uttam Malunje
Student, GCE, Karad
Karad, India
Uttam4n@gmail.com

Mr.Sajjan Mane
Student, GCE, Karad
Karad, India
sajjanmane@gmail.com

Abstract— **In cloud computing, data is transferred to a closest server from the owner. The major task of this Cloud Server (CS) is to store the data and return it on demand of the owner of the data. The Cloud Server contains the data from various Clients. Thus, data integrity is one of the important issues of the Cloud Server. After storing the data on the Cloud Server, user hopes that the data and the application are protected just like the data on his location. But there are chances that the owner's data may be altered or deleted due to any reason. In this scenario, the user needs to download the data in order to validate it. This data can be very large file, downloading such large file to check the data integrity should be prohibited as it requires large bandwidth and time. If this validation need to be performed frequently then this process is not feasible. This project propose a method which does not require to download files to check the data integrity and it provides a way to store and maintain the data on the Cloud Server. Data at a remote storage in cloud is not modified by anyone and there by integrity of the data is assured. Because data integrity ensured that data is of high quality, correct, consistent, and accessible. Data owner can resort to a Third Party Auditor (TPA) to check the integrity of data stored in cloud server. Thus we introduce a TPA which audits and maintain the data on Cloud Server and used RSA algorithm for encryption and HLA for auditing.**

Keywords— Third Party Auditor (TPA), cloud server (CS), cloud user (U), RSA algorithm, HLA algorithm.

I. INTRODUCTION

"Cloud" is a buzzword [1] which often refers to the Internet and more precisely to some data centre full of servers that is connected to the Internet. Cloud computing is defined as a type of computing that is depended on the sharing of computing resources rather than having local servers or personal devices to handle applications. It provides an on-demand access to the shared resource present on the Cloud Server. These Shared resource are networks, servers, storage, applications, and services that can easily managed for user by the service provider. This cloud model promotes availability of data and service by the help of five essential characteristics (integrity, security, authentication, privacy and availability), three service models (IaaS, PaaS, SaaS), and four deployment models [1] (Public, Private, Community and Hybrid Cloud).

Whenever user stores the pictures online instead of keeping it on his/her own personal computer, at that moment the user is using a "cloud computing" service. Cloud computing provides the computing services over the Internet. Cloud services are available to individuals and businesses to use software and hardware that are managed by third parties at remote locations. Some of the examples of cloud services are storing files on Google drive or Dropbox, social networking websites like Facebook, Twitter, use of electronic mail, and many applications and software available on the internet like office online by Microsoft. Also accessing the information and resources from any place where a connectivity of network is available. Cloud computing provides a lake of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications which is available to users as per request.

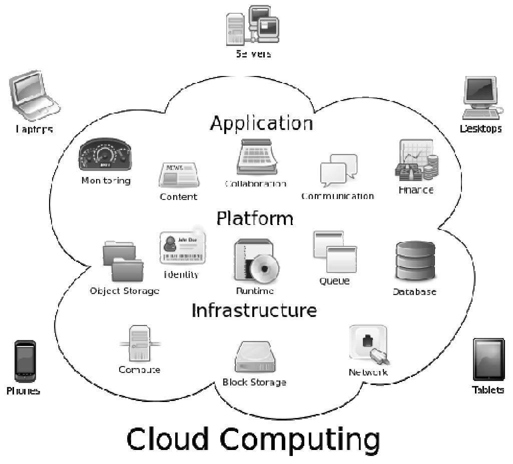


Fig 1: Overview of cloud computing

A. Cloud Storage:

Cloud storage is storing data on the cloud or online instead of storing [1] on the personal computer. The data of different companies are stored on different places which are distributed and connected to each other under the cloud computing scenario and also make available at any place where the network connectivity is possible. Cloud storage[2] has great advantages such as easy access and reliability; fast deployment; higher security for backup data and cost effective as a result of not having to purchase, managing and maintaining expensive hardware. After words, cloud storage does have provides security and compliances.

There are several advantages of using cloud storage, mostly want to mention that is accessibility of data or file like document, images, and music files. We can access files which are stored on the cloud storage from any location and any time when we want, but with the still connected to Internet. Another one is that cloud storage providing facility for off-site (remote) backups of data available to organizations which reduces costs required to disaster recovery. Unfortunately, the biggest disadvantage to cloud storage is that users can not cross the bandwidth limit. Suppose, if you have slow or unstable Internet connection, you might have face to problems while accessing the data from cloud storage. Some of the organizations requires large amount of storage space that may be increase the cost significantly after the first few gigabytes of data stored.

B. Cloud Security Issues:

Organizations use the Cloud in a variety of different service models such as SaaS,PaaS, and IaaS; and deployment models which are Private, Public, Hybrid and Community. There is number of security issues associated with cloud computing but these issues fall into two broad categories [3]:

- Security issues faced by cloud providers which are providing services in the sense of software, platform, or infrastructure by using cloud and
- Security issues which are faced by cloud users like companies or organizations who host applications or store data on the on the cloud.

Responsibility of service provider is to keep track of data security with integrity; also it is the responsibility of client or cloud user to keep strong password with confidentiality.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity [3].

In order to conserve resources, cut costs, and maintain efficiency [4], Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation [4] and logical storage segregation

II. OBJECTIVE

The objective of this project is to provide the security for the data that are stored in the cloud environment using privacy-preserving public auditing mechanism, and so that we can increase the security level for the data that are stored in the cloud servers..

III. LITERATURE REVIEW

K. Meenakshi proposes a method that, owner need not download the data or files to check the integrity and it provides the proofs that data is stored at a remote storage in cloud is not modified by anyone and there by integrity of the data is assured. Because data integrity ensured that data is of high quality, correct, consistent, and accessible. Data owner can resort to a Third Party Auditor (TPA) to check the integrity of data stored in cloud server.

Imran Ahmad proposed a secure cloud storage system supporting privacy-preserving public auditing. Also further extend result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Security and performance analysis shows the proposed schemes are secure and proficient. Experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

Miss. Nupoor, M. Yawaleproposes a secure cloud storage system supporting privacy-preserving public auditing and further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently with RC5 Encryption Algorithm. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

IV. PROBLEM STATEMENT

Cloud storage has been envisioned as the next-generation architecture of IT Enterprise cloud computing. But, the data here may not be completely reliable. Here data is in large data centres, which contain data of various customers and it can be accessed by them anytime. So most important task is ensuring the integrity of the data.

In cloud computing services not pressurizing on the backup of data while the changing the block by inserting or removing operation of data. These are supports for dynamic data which is an important for reality. Making data update dynamically with identifying security problems

V. SYSTEM ARCHITECTURE

A cloud data storage service involving three different entities [5].

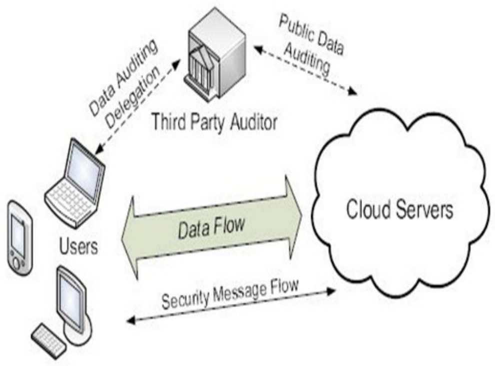


FIG 2: SYSTEM ARCHITECTURE OF CLOUD SYSTEM

- The cloud user (U): who has large amount of data files to be stored in the cloud.
- The cloud server (CS): This 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): has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

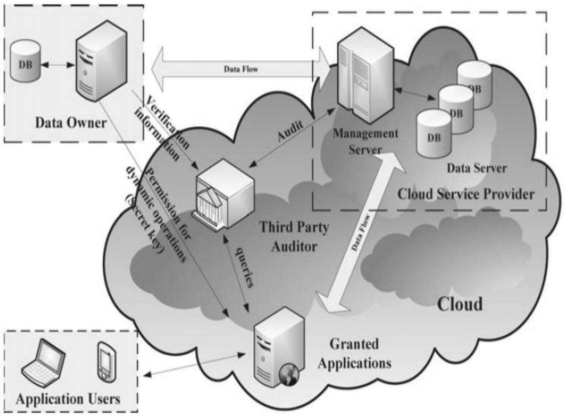
A. AUDIT SERVICE SYSTEM

An audit is an evidence gathering process [5]. Audit evidence is used to evaluate how well audit criteria are being met. Audits must be objective, impartial, and independent, and the audit process must be both systematic and documented.

Auditor

An auditor is a person who carries out audits. Auditors collect evidence in order to evaluate how well audit criteria are being met. They must be objective, impartial, independent, and competent.

Fig 3: Audit system architecture for cloud computing



*Third party auditor (TPA):*Who has capabilities to manage or monitor outsourced data under the delegation of data owner [6].

*Criteria for auditing:*Criteria used for auditing of data are:

- By Size: Size of the file.
- By Format: Format of the file.
- By Modify time: last modified time of the file.
- By Access time: last access time of the file.
- By Download: no of time file downloaded

VI. Algorithms

[1] RSA ALGORITHM

Use: RSA algorithm using for the authentication purpose.

Concept:

RSA [7] involves a public key and a private key.The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q. (For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.)

2. Compute n = pq. (n is used as the modulus for both the public and private keys).

3. Computeφ(n) = (p – 1)(q – 1), where φ is Euler's totient function.

4. Choose an integer e such that 1 < e <φ(n) and greatest common divisor of (e, φ(n)) = 1; i.e., e and φ(n) are coprime. (e is released as the public key exponent).

5. Determine d as:

$$\mathbf{d = e^{-1}(mod(\varphi\ (n))}$$

i.e., d is the multiplicative inverse of e mod φ(n).

*ENCRYPTION:*Encryption is the process of converting plain text into cipher text.

$$\mathbf{C = m^{e}(mod\ (n)\ )}$$

*DECRYPTION:*Decryption is the process of converting ciphertext into plain text**.**

$$\mathbf{m = c^{d}(mod(n))}$$

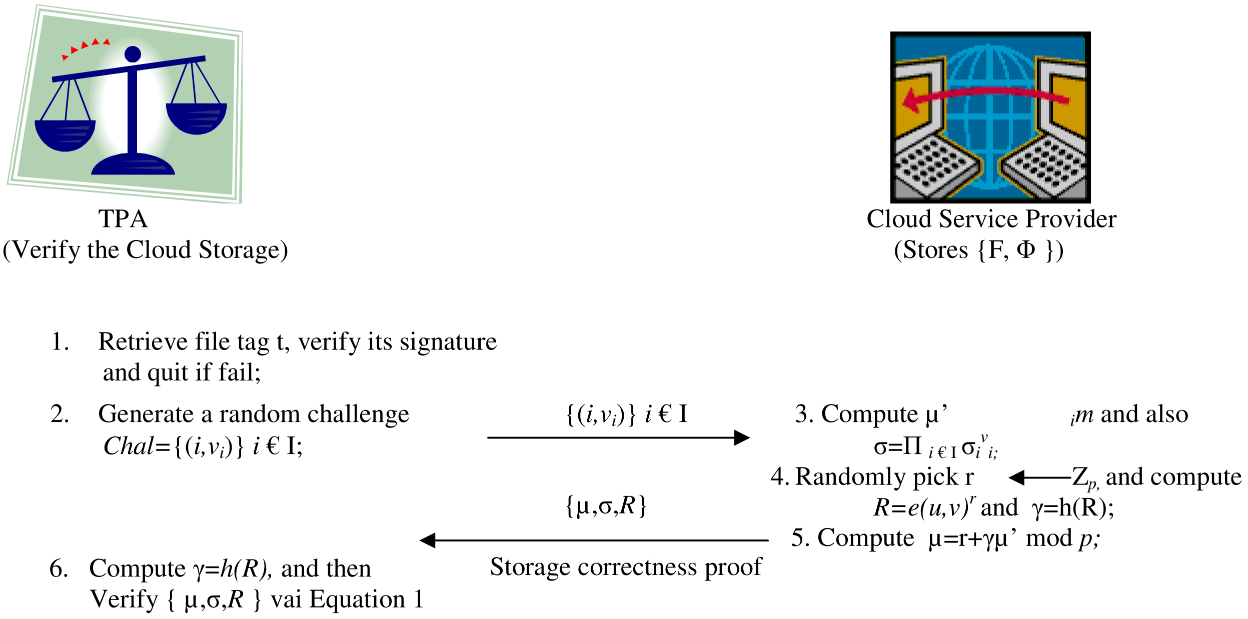
[2] HLA based ALGORITHM

Use**:** HLAalgorithm using for checking integrity of data blocks.

Concept**:**

To effectively support public audit ability without having to retrieve the data blocks themselves, the HLA [8] technique can be used. It is possible to compute an aggregated HLA which authenticates a linear combination of the individual data blocks. At a high level, an HLA-based proof of storage system works as follow. The user still authenticates each element of F = {mi} by a set of HLAs φ .The TPA verifies the cloud storage by sending a random set of challenge {vi}. The cloud server then returns $\boldsymbol{\mu=\sum_i v_i m_i}$and its aggregated authenticator**σ**computed from φ. Though allowing efficient data auditing and consuming only constant bandwidth, the direct adoption of these HLA based techniques is still not suitable for our purposes. This is because the linearcombination of blocks, $\boldsymbol{\mu=\sum_i v_i m_i}$may potentially reveal user data information to TPA, and violates the privacy-preserving guarantee. Specifically, by challenging the same set of c block m_1,m_2,m_3...........m_c using c different sets of random coefficients $\{v_i\}$.TPA can accumulate c different linear combinations u_1,.......u_c. With $\{u_i\}$ and $\{v_i\}$, TPA can derive the user's data m_1,m_2,.....m_i by simply solving a system of linear equations.

The TPA verifies the cloud storage by sending a random set of challenge $\{v_i\}$. The cloud server then returns μ= and its aggregated authenticator σcomputed from φ. Though allowing efficient data auditing and consuming only constant bandwidth, the direct adoption of these HLA based techniques is still not suitable for our purposes. This is because the linear combination of blocks,μ= may potentially reveal user data information to TPA, and violates the privacy-preserving guarantee.



1. Retrieve file tag t, verify its signature and quit if fail;
2. Generate a random challenge $Chal=\{(i,v_i)\}$ i € I;

3. Compute μ' $_i m$ and also $\sigma=\Pi_{i € I}\sigma_i^{v}{}_{i;}$
4. Randomly pick r ⟵ $Z_{p,}$ and compute $R=e(u,v)^r$ and γ=h(R);
5. Compute $\mu=r+\gamma\mu'$ mod $p;$

6. Compute $\gamma=h(R),$ and then Verify { μ,σ,R } vai Equation 1

Specifically, by challenging the same set of c block m_1,m_2,m_3...........m_c using c different sets of random coefficients $\{v_i\}$.TPA can accumulate c different linear combinations u_1,.......u_c. With $\{u_i\}$ and $\{v_i\}$, TPA can derive the user's data m_1,m_2,.....m_c by simply solving a system of linear equations.

VI. Conclusion

We propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator and RSA algorithm to guarantee that the 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, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

VII. References

[1] Cloud Computing by Margaret Rouse www.searchcloudcomputing.techtarget.com/definition/cloud-computing

[2] CloudStorage,http://www.webopedia.com/TERM/S/storage_cloud .html

[3] Cong Wang, Sherman S.M.Chow, Qian Wang, KuiRen, and Wenjing Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE , Vol.62 , No. 2,February 2013..

[4] C.Wang, Q.Wang, K.Ren, and W.Lou, "Privacy Preserving Public Auditing for Storage Security in Cloud Computing", IEEE INFOCOM'10, March2010.

[5] Imran Ahmad "Privacy-Preserving Public Auditing & Data Intrgrity for Secure Cloud Storage", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV.

[6] Miss. Nupoor M. Yawale Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm

[7] HLA Based Third Party Auditing For Secure Cloud Storage, ChandineeSaraswathyK. ,Keerthi D. Padma G. Student , Department of Computer Science and Engineering Velammal Institute of Technology, Panchetti.

[8] A.Nath, S.Ghosh, M.A.Mallik " Symmetric key cryptography using random key generator", Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July,2010, Vol-2,P-239-244.

[9] Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, Journal Computing Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm, , Vol.3, issue 2, Page 66-71,Feb 2011.

[10] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath :"A new Symmetric key Cryptography Algorithm using extended MSA method DJSA symmetric key algorithm", accepted for publication in IEEE CSNT- 2011 to be held at SMVDU(Jammu) 03-06 June 2011.

[11] William Stallings “Cryptography and Network”, Prectice Hall of India

[12] http://e.wikipedia.org/wiki/Performance Analysis of Data Encryption Algorithms.html

[13] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[14] http://en.wikipedia.org/wiki/Data_Encryption_Standard

[15] http://en.wikipedia.org/wiki/Triple_DES

[16] http://www.splashdata.com/splashid/blowfish.htm

[17] https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Data_Encryption_Standard.html