Multi-User Setting For Dynamic Data Invocation for Privacy-Preserving In Public Cloud Storage

K. Sathish [1], Y. Jansi, M.Tech[2], Dr. M. Giri, M.Tech,Ph.D [3]
M.Tech Scholar, Assistant professor, Professor & Head, Department of C.S.E
[1,2,3]Department of Computer Science and Engineering Sreenivasa Institute of Technology and Management Studies Chittoor, Andhra Pradesh, India

***Abstract**: Cloud Computing is an latest up growing technology which provide various services to internet, it enables to store the data in to a cloud storage and the on demand scalable services. The users should use the cloud storage data as it is local without verifying its integrity and correctness of data. The public auditing for cloud storage is important, so that to check the integrity of outsourced data in the cloud, the users will take the action to check the integrity of data in a Intermediate Cloud Accessor (TPA) . To securely introduced an effective Intermediate Cloud Accessor (TPA), the auditing processor should bring an new concerns for user data privacy, for that the watermarking for data storage security in cloud computing is proposed. It supports data dynamics where users can perform various operations on data like insert, update and delete as well as batch auditing where multiple user request for storage correctness will be handled simultaneously which reduces the communication and computing cost.*

***Index Terms**: Privacy preserving, public auditing, watermarking, Intermediate Cloud Accessor (TPA), Security.*

I. Introduction:

Cloud computing is using hardware and software has computing resources to provide service through internet. Cloud computing has many advantages as follows it can upload an download data stored in the cloud without concern about security. It can access the data from anywhere any time on demand and cost is low or paper usage. Hardware and software resources are easily without location
independent, the major disadvantages of cloud computing is security.

1.1 Security Issues:

The security is a major issue in cloud computing. It is a sub domain of computer security, network security or else data security. The cloud computing security refers to a broad set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud
computing. Some security and privacy issues that need to be considered are as follows

1) Authentication*:* Only authorized user can access data in the cloud

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure.

3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data.

4) No storage Overhead and easy maintenance**:** User doesn't have to concern about the storage requirement & maintenance of the data on a cloud.

5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.

6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation.

In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without concern about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done.

Security in cloud computing can be addressed in many ways as authentication, integrity, confidentiality. Data integrity or data correctness is another security issue that needs to be considered. The proposed scheme specifies that the data storage correctness can be achieved by using SMDS (Secure Model for cloud Data Storage). It specifies that the data storage correctness can be achieved in 2 ways as 1) without trusted third party 2) with trusted third party based on who does the verification.

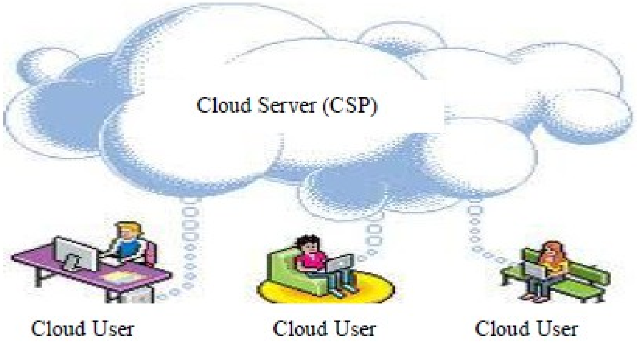

Fig 1: Cloud Architecture

It provides data confidentiality in two stages as 1) Data at rest 2) Data in transmission.
1. Data at rest: Symmetric key encryption technique(i.e. AES, TDES, and DES) are recommended which are secure but more time consuming.
2. Data in transmission: Secure Socket Layer (SSL) protocol is used for integrity verification. It uses a two different hash function such as Secure Hash Algorithm (SHA1) for digital signature and Message Digest (MD5) is a cryptographic hash function which is used to check the data integrity.

To achieve storage correctness without trusted Intermediate cloud accessor (TTP), it has major goals in proposed schemes.

- CS neither should learn any information from user’s data nor should misuse the same.
- The User selects the encryption option for their data
- Secure key management
- Flexible access right managements
- It aims to achieve light weight integrity verification process for checking the unauthorized change in the original data without requesting a local copy of the data.

It uses public key encryption to encrypt the data to data storage correctness. It achieves the following goals as data confidentiality, security, light weight verification, key management, access right and no data duplication.

The correctness of data can be violated due to a broad range of both internal and external threats and CSP may hide data loss or damage from users to maintain a reputation. Major security issues associated with cloud user and CSP are as follows
1) Cloud Service Provider (CSP): Organization or enterprises provide various services to cloud users. Confidentiality and integrity of cloud data should be maintained by CSP. The Provider should ensure that user’s data and application are secured on a cloud. CSP may not leak the information or else cannot modify or access user’s content. The attacker can log into network communication.
2) Cloud Server (CS): The cloud server where data being stored and accessed by cloud data owner or users. Data should not be accessed by unauthorized users, no data modification or no loss of data.
3) Cloud User: Attackers can access basic information like username and password. Key management is major issue in encryption techniques. Data dynamic issues need to be considered by CSP.
Cloud Computing Threads are as follows:

1. Spoofing Identity Theft
2. Data Tempering Threat
3. Repudiation Attack
4. Information Disclosure on up/download Intra-Cloud
5. Denial of Service Attack
6. Log In

To achieve the security, for a data to a third outsourced party who will specify the correctness and integrity of the cloud data. An intermediate cloud accessor (TPA) is proposed, who will audit the user data stored on the cloud, based on the users request.

In Cloud service provider doesn’t have to concern about the correctness and integrity of the data. In this technique, Intermediate cloud Accessory will audit the cloud data to check the integrity or correctness in two ways as: 1) Download all files and data from the cloud for auditing, it include I/O and network transmission cost. 2) Apply auditing process only for accessing the data but the data loss or data damage cannot be defined for un accessed data. Public audit ability allows user to check integrity of outsource data under different system & security models. It cannot achieve privacy as Intermediate cloud Accessor can see the actual content stored on a cloud during the auditing phase. Intermediate cloud Accessor itself may leak the information stored in the cloud which violate data security. To avoid this, Encryption technique is used where data is encrypted before storing it on the cloud.

II. The System And Thread Model

The cloud data storage service contains 3 different entities as cloud user, Intermediate cloud Accessor & cloud server / cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is a place where is to stored the cloud data and that data will be managed by the cloud service provider. Intermediate cloud Accessor will do the auditing on users request for storage correctness and integrity of data.

The proposed system specifies that user can access the data on a cloud as if the local one without concern about the integrity of the data. Intermediate cloud Accessory(TPA) is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

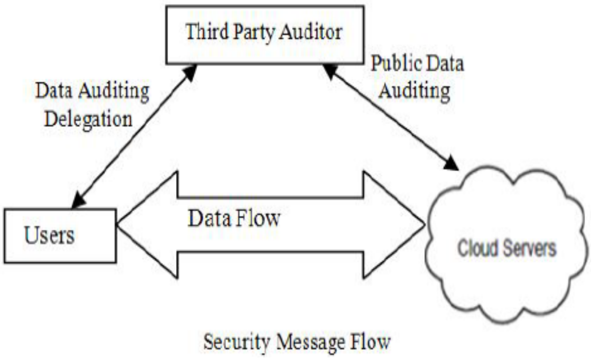

Fig 2 : Architecture Of Cloud Data Storage Service

Intermediate cloud Accessor (TPA) checks the integrity of the data stored on a cloud but if the Intermediate cloud Accessor (TPA) itself leaks the user’s data. The new concept comes as auditing with zero knowledge privacy where Intermediate cloud Accessor (TPA) will audit the users’ data without seeing the contents. It uses public key based homomorphic linear authentication (HLA), Intermediate cloud Accessor (TPA) allows to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow Intermediate cloud Accessor (TPA) to learn data content. It uses encryption technique to encrypt the content of the file.

A. Goals

 It allows TPA to audit users’ data without knowing data content.

 It supports batch auditing where multiple user requests for data auditing will be handled simultaneously.

 It provides security and increases performance through this system.

B. Design Goals

1) Public audit ability: Allow Intermediate cloud Accessor (TPA) to check data correctness without accessing local data.
2) Storage Correctness: The data stored on a cloud is as it. No data modification is done.
3) Privacy preserving: Intermediate cloud Accessor (TPA) can’t read the users’ data during the auditing phase.
4) Batch Auditing: Multiple users auditing request is handled simultaneously.
5) Light Weight: Less communication and computation overhead during the auditing phase.

C. Batch Auditing:

It also supports batch auditing through which efficiency is improved. It allows Intermediate cloud Accessor (TPA) to perform multiple auditing task simultaneously and it reduces communication and computation cost.

D. Data Dynamics

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. In proposed scheme which support simultaneous public audability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It uses MHT for block tag authentication.

III. Intermediate Cloud Accessory (TPA) Data Storage Security Scheme For Public Auditing

A. MAC Based Solution

It is used to authenticate the data.The user upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Problems with this system are listed below as

1. It introduces additional online burden to users due to
2. Limited use (i.e. Bounded usage) and stateful verification.
3. Communication & computation complexity
4. Intermediate cloud Accessor (TPA) requires knowledge
5. of data blocks for verification
6. Limitation on data files to be audited as secret keys are
7. fixed
8. After usages of all possible secret keys, the user has to
9. own load all the data to recomputed MAC & republish it
10. on CS.
11. Intermediate cloud Accessor (TPA) should maintain &
12. update states for Intermediate cloud Accessor (TPA)
13. which is very difficult
14. It supports only for static data not for dynamic data.

B. HLA Based Solution

It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth. It is possible to compute an aggregate HLA which authenticates a linear combination of the individual data blocks.

C. Privacy Preserving Public Auditing Is Proposed

Public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows Intermediate cloud Accessor (TPA)to do auditing without requesting for local copy of the data. Through this scheme , Intermediate cloud Accessor (TPA) can audit the data and cloud data privacy is maintained. It contains 4 algorithms as

1) Keygen: It is a key generation algorithm used by the user to setup the scheme.
2) Singen: It is used by the user to generate verification metadata which may include digital signature.
3) GenProof: It is used by CS to generate a proof of data storage correctness.
4) Verifyproof: Used by Intermediate cloud Accessor (TPA) to audit the proofs It is divided into two parts as setup phase and audit phase.

1) Setup Phase: Public and s parameters areinitialized by using keygen and data files f are preprocesses by using singen to generate verification metadata at CS & delete its local copy. In preprocessing user can alter data files F.

2) Audit Phase: TPA issues an audit message to CS. The CS will derive a response message by executing Genproof. TPA verifies the response using F and its verification metadata.

Intermediate cloud Accessor (TPA) is stateless i.e. no need to maintain or update the state information of audit phase. Public key based homomorphic linear authentication with random masking technique is used to achieve privacy preserving public auditing. Intermediate cloud Accessor (TPA) checks the integrity of the outsourced data stored on a cloud without accessing actual contents. Proofs of Data Possession (PDP) technique doesn't consider data privacy problem. PDP scheme first used to detect large amount corruption in outsourced data. It uses RSA based Homomorphic authentication for auditing the cloud data and randomly sampling a few blocks of files. A Second technique is used to Proofs of retrievability (PoR) allows user to retrieve files without any data loss or corruptions. It uses spot checking & error correcting codes are used to ensure both "Possession" and "Retrievability". To achieve Zero knowledge privacy.

D. Virtual Machine

Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions . The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency.

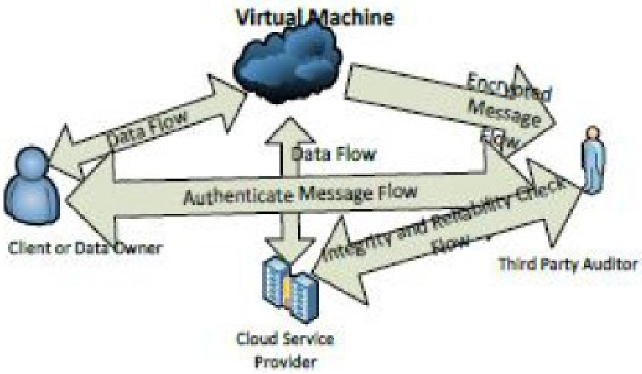

Fig 3: Architecture Of Cloud Server With CU and TPA

E. Random Masking Technique

Privacy preserving Intermediate cloud Accessor without data encryption. It uses a linear combination of sampled block in the server's response is masked with randomly generated by a pseudo random function (PRF).

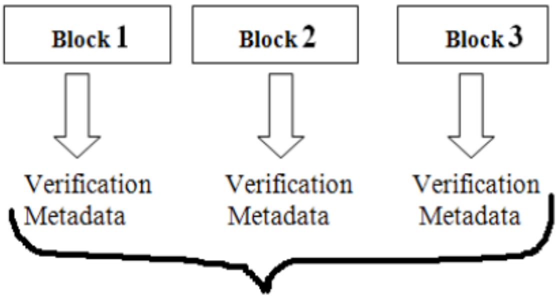

Fig 4 : Homomorphic Authenticator

The concept of virtual machines, The RSA algorithm is used to encode and decode the data. A new password is generated at each instance which will be transferred to the mail server for each request to obtain data security and data integrity of cloud computing. This protocol is secure against an untrusted server as well as intermediate cloud accessor. Client as well as trusted intermediate cloud accessor verifier should be able to detect the changes done by the intermediate cloud accessor. The client data should be kept private against intermediate cloud accessor verifier. It supports public verifiability without help of a intermediate cloud accessor. This protocol does not leak any information to the intermediate cloud accessor verifier to obtain data security. This proposed protocol is secure against the untrusted server and private against third party verifier and support data dynamics. In this system, the password is generated and that will be transferred to email address of the client. Every time a key is used to perform various operations such as insert, update delete on cloud data. It uses time based UUID algorithm for key generation based on pseudo random numbers. If an intruder tries to access the users' data on a cloud, that IP address will be caught and transferred to the user so that user will be aware of.

F. Security Flaws For This Protocol

To find the security flaws in the protocol, a public auditing protocol is a collection of four polynomial time algorithm as (Keygen, TagBlock, Genproof, and CheckProof)
Keygen: User executes Keygen for key generation.
TagBlock: User executes TagBlock to produce verification metadata.
Genproof: Cloud server executes Genproof for proof of possession.
CheckProof: TPA will validate a proof of possession by executing CheckProof.
The Problem with this system is that cloud server might be malicious which might not keep data or might delete the data owned by cloud users and might even hide the data possessions.

1) Data modification tag forging attacks
2) Data lost auditing pass attack
3) Data interception and modification attack
4) Data Eavesdropping and Forgery

This protocol is vulnerable to existential forgeries known as message attack from a malicious cloud server and an outside attacker. The analysis shows that they are not providing any security for cloud data storage.

IV. Proposed Scheme

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material . And provide additional security such as watermark technique at specific time interval. These techniques enable single sign-on in the cloud and access control for sensitive data in both public and private clouds.

In the Proposed system the water marking process, to store the data or images in the cloud server by assigning the public key, and this key and watermarking images are sent to and third party have complete authority to check the key and sent it to the server, and there intermediate cloud accessor must have a public key whenever the data to be retrieved. In the watermarking process, the security level is very high so the data or images cannot be identified by the attackers in the cloud. We also uses Compression technique for watermark image to reduce communication overhead.

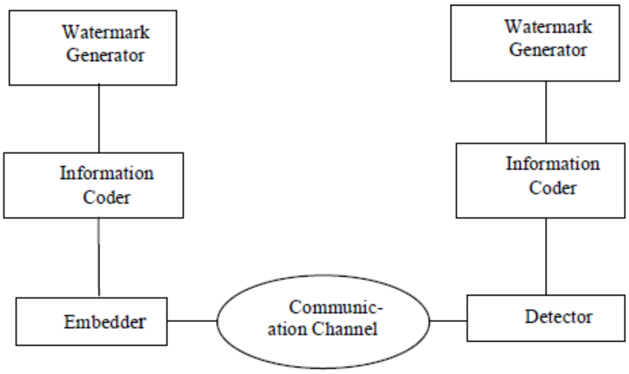

Fig 5:Watermarking technique

The main elements in watermarking process: an embedded, a communication channel and a detector and is shown in Figure. Watermark information is embedded into original image itself, and it is performed in the encryption process for making security on original information. Embedded is similar to encryption process which is used to change content into another format with the help of the secret key. Detector process is also similar to decryption process which is used to perform reverse process of encryption. The watermark information is embedded within the original image before the watermarked image is transmitted over the communication channel, so that the watermark image can be detected at the receiving end.

V. Conclusions

The watermarking technique for Privacy Preserving Public Auditing for cloud data storage security is proposed. Cloud computing security is a major issue that needs to be considered**.** Using TPA, it can verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security. To achieved zero knowledge privacy through rando masking supports batch auditing where intermediate cloud accessor (TPA) will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing. It also supports data dynamics. It uses Merkle Hash Tree (MHT) for it. Privacy Preserving Public Auditing with watermark process for secure cloud Storage is introduced**.**

References

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing,” Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. Html, 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[3] M.Arrington,“Gmail disaster: Reports of mass email deletions,” Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.

[4] J.Kincaid,“MediaMax/TheLinkup Closes Its Doors,” Online at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[5] Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[6] S. Wilson, “Appengine outage,” Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008.

[7] B. Krebs, “Payment Processor Breach May Be Largest Ever,” Online at http://voices.washingtonpost.com/securityfix/ 2009/01/payment processor breach may b.html, Jan. 2009.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

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

[10] 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.