Auditing Mechanism for Ensuring Data Storage Security in Cloud Computing

J.Aparna
PG Student of CSE
Madanapalle Institute of Technology & Science
JNTUA University, Anantapur
Andhra Pradesh, India

R.Sathiyaraj
Department of Computer Science & Engineering
Madanapalle Institute of Technology & Science,
JNTUA University, Anantapur
Andhra Pradesh, India

ABSTRACT
Now a day's most of the firms are shown interested to place their data in a cloud based networks because of its utilities and problems with traditional data storage tools. If we are storing data outside of its environment means outsourced it leads to privacy issues. Also considerable factor is that security here users worried about integrity and accountability. Security is a considerable issue for this type of data centers. Security consist set of policies, applications and infrastructure. In this project we propose a model to overcome these issues, outsourced data are verified by trusted third party persons to ensure its integrity. This auditing was done because most of the data's are outsourced. Next it will be focused on security and performance analysis issues this was done by auditors simultaneously without over burden to the users.

Keywords
public audit ability, privacy-preserving, cryptographic protocols, cloud computing, Data storage

1. INTRODUCTION
CLOUD computing have be envision like the next invention information technology (IT) structural design for enterprise, owing to its lengthy catalog of extraordinary compensation in the IT record: on demand identity service, everywhere system access, position self-governing resource pool, rapid store flexibility, usage based price and transfer of threat. The same as a troublemaking skill with thoughtful implication cloud computing is transform the incredibly character of how business use IT. Single elementary feature of this archetype changing is to information be organism regional before outsourced to the confuse storage. As of user point of view, together with mutual persons with IT enterprise, store information distantly to the cloud within a supple on order method bring interesting profits: release of the load for storage managing, entire information accessing by location self-determination, and prevention of resources expenses on hardware, software, and human resources maintenance, etc., whereas cloud compute make these compensation more interesting than ever, it as well bring new and demanding security pressure toward user outsourced information. Ever since cloud service providers (CSP) are different organizational entities, data outsourcing is actually relinquished user's crucial manage over the destiny oftheir Information. The same as a outcome, the appropriateness of the information in the cloud is being put at possibility due to the next reason. Firstly, though the framework in the clouds is very much more great and consistent than individual compute procedure, they are immobile face the wide range of both external and internal pressure for information reliability. Example of outages and protection breach of notable cloud service come out from time up to date. Next, these do survive various motivation for cloud service provider to perform falsely toward the cloud user as regards their outsource information kind. For example, cloud service provider might retrieve storage space for economic reason by throwing away information that have not be or are infrequently access, or constant hides information lost incident to sustain a repute. In brief, though outsourced information to the cloud is inexpensively gorgeous for long term large scale storage, it doesn't instantly propose any assurance on data reliability and accessibility. That complexity, if not accurately address, may obstruct the success of cloud structural design.

Since users no longer actually acquire the storage of that information, conventional cryptographic primitive for the reason of information security defense can't be straight adopt. During exacting, basically downloads all the information for it's reliability authentication is not a useful solutions suitable to the expensiveness in Input Output and communication expenses across the system.

Further, that is continually inadequate to determine the information correctness only while accessing the information, as it does not gives user accurateness maintain for that un accessed information and may be too overdue to recovering the data lost or damages. Assume the huge volume of the outsource information and the users confine source capacity, the responsibilities of audit the information correctness in a cloud location should be horrible and more costly for the cloud user. As well, in the clouds of usage of cloud storage space can be decrease as possible, for this a user doesn't require to do too many number of tasks to using the data. Specially, user might not to go throughout the difficulty in verify the data consistency. Additionally may be there more number of users access the similar cloud storage space, articulate in an activities settings. For easy managing, that is attractive this cloud only entertain authentication demand from a one preferred party.

The aggregation and geometric property of the authorized user additional advantage our plan for the batch auditable process. Specially, our involvement can be summarizing as the follow three aspects:

1. Inspire the free auditable organization of information storage space protection in the cloud compute and providing a Auditing mechanism for secure cloud storage. Our method allows outside auditor to auditing the user cloud information without learn the information's contented.

2. For the most of our information, our method is the first to supporting scalable and capable auditable method for out sourced cloud storage space.

3. Here we express the protection and validate the performance of our anticipated scheme during concreted experiment and comparison with the time to time.

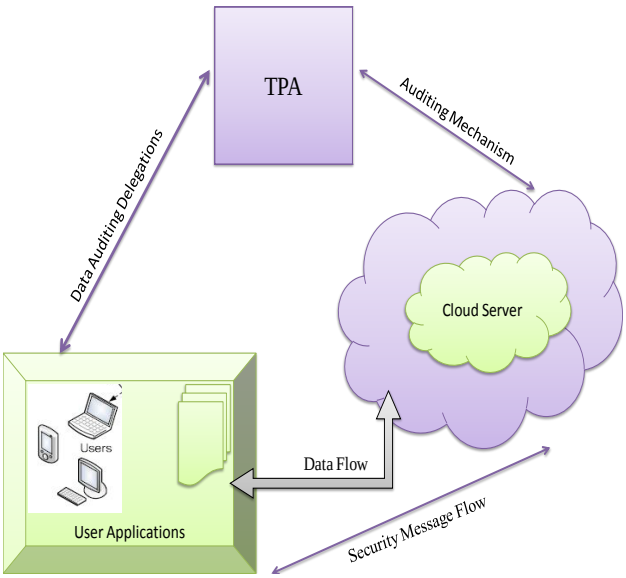
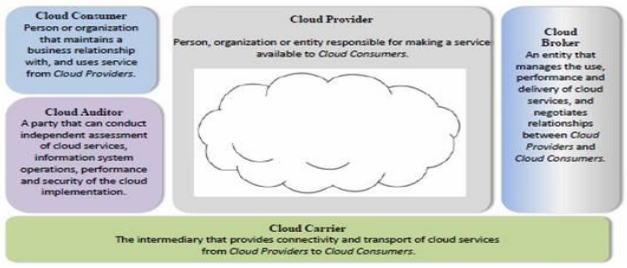


Fig1. The Design of Auditing mechanism for Ensuring Data Storage in Cloud Computing

2. RELATED WORK

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple clouds other over application programming interfaces, usually web services.



Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture fig1 is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or user.

1) Proc. IEEE INFOCOM '10, Mar. 2010, K. Ren and W.Lou, , C.Wang, Q. Wang, K. Privacy-Preserving Public Auditing for Storage Security in Cloud Computing Ren and W.Lou,

Cloud compute is the wide-ranging dreamed visualization of compute as a consequence, everywhere user be able to indistinguishably accumulate that information into the cloud so that have the on demand high excellent application and services from a general mere of configurable compute resource.

From information outsourcing, user is able to at ease from the consignment of local information storage and protection. Whereas, the information that user no longer contain forcibly controlling of the maybe huge size of outsourced information make the data accuracy security in Cloud Computing a extremely challenging and potentially sound the alarm mission, predominantly for user among constrain computing possessions and capability. For that reason, enable public audit ability for cloud information storage protection is a significant implication so these users be capable to choice to an outside audit party to validate the consistency of outsourced information when required.

To confidently fetch in an effective third party auditor (TPA), the subsequent two essential materials contain that are:

1. TPA should be accomplished to professionally audit the cloud information storage exclusive of durable the local copy of information, and carry in no accompanying online load to the cloud users.

2) The thirdpartyaudit system must convey in no new vulnerabilities towards users information confidentiality. We make use of and absolutely come together the public key base homomorphic authenticator through unsystematic mask to achieve the privacy preserve public cloud information auditing system, which gather all above necessities. To sustain capable handle of multiuser auditable responsibilities, we additional survey the method of bilinear combined signatures to enlarge our main consequence into a multiuser settings, here TPA be able to execute multiple auditable responsibilities concurrently. Extensive protection and presentation study show the anticipated scheme are provably protected and extremely capable.

2) http://status.aws.amazon.com/s3-20080720.html, Amazon.com, Amazon s3 Availability Event: July 20 ,2008, July 2008

Throughout the increasing of framework infrastructure, the concentration in outsourcing the essential system services is increase. In science grids, information storage space is individual such essential services : certainly, in many organizations terabytes of latest information are formed every day and to a large extent more is process. recently, Amazon.com have introduces a description storage convenience, the SimpleStorageService (3S). 3S aim to give data storage as a low-cost, extremely accessible service, with simple pay-as-you-go bill representations. That objects evaluate 3S as a black box and reason whether 3S is an appropriate service for science grid. In these procedure, it's identify materials for a storage services intended for this exacting kind of civilization, with security feature and a extra expand collection of storage possessions with different capability and a additional flexible price system.

3) IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp.Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, May 2011, 847-859.

Cloud Compute has been envisioning the same as the next production construction of information scheme. It progress the application software and database into the central huge information center, wherever the organization of the

information and services might not be totally responsible. That single illustration brings on lots of new protection challenge, which hasn't been fine unspoken. These work study the troubles of ensuring the integrity of information storage space in Cloud compute.

In difficult, we are thinking the tasks of allow a third party auditor (TPA), on half of the cloud customer, by validate the integrity of the active information stored into the clouds. These introduction of Third Party Auditor eliminate the involvement of the user during the audit of whether his information store into the clouds are certainly complete, which know how to be significant to achieve economy of range for Cloud Compute.

The broadcasting for information dynamics by way of the most common form of information procedure, such the same as building block adaptation, addition, and removal, it is also a major step in the direction of reasonableness, ever since service in Cloud Compute are not unfinished the report or endorsement information only. Whereas previous workings on ensure distant information reliability a lot lack the maintain of moreover public auditing or else self-motivated information operations, achieve together. Here first we identify the difficulty and achievable protection troubles of directly extension among completely active information update as of preceding workings after that illustrate how to construct a neat confirmation method used for the perfect incorporation of this mainly significant features in this proposed method.

3. EXISTING METHODOLOGY

In the Existing method, the concept of public audit ability has been anticipated in the framework of ensure distantly stored information reliability in special method and security model. Public audit ability allows an outside gathering, in adding to the users himself to validate the accuracy of distantly stored information. Though, mainly of this scheme doesn't reflect on the confidentiality security of user data beside outside auditor. Certainly, they might potentially make public user data to auditor. Such cruel problem affects the protection of these protocol in cloud computing. since the point of view of protected data confidentiality, the user, who have the information and rely on TPA now for the storages protection of their data, don't desire this audit procedure introduce latest damages of illegal data leak to their information security.

3.1 Limitations of Existing Method

Even though the infrastructures below the cloud are greatly further influential and consistent than individual computing procedure. Encryption doesn't totally solve the difficulty of protective information confidentiality beside the third party auditor.

4. PROPOSED METHODOLOGY

In this project, we use the public key base homomorphism authenticator and uniquely integrated. By this random mask techniques to attain an Auditing mechanism for outsourced cloud storage, whereas all above mentioned necessities in considerations. To sustain capable handle of several auditable responsibilities, In addition, we search the techniques of bilinear aggregation signatures to extend our major results into a multiple user's settings, wherever TPA can perform multi auditing responsibilities concurrently. Generally protection and presentation study shows the future schemes are provably make safe and highly efficiency. Here we also explain how to exposure our major schemes to support multiple tasks to TPA from delegation for batch auditing.

The following are the proposed methods that are used for Auditing mechanisms for outsourced cloud storage.

- Isolated information reliability examination protocol for cloud storages. The future scheme inherits the maintenance of information dynamics, and supports public verifiability and isolation beside third party verifiers, although at the same time it doesn't require to utilize a third party auditor.
- Protection study of the proposed systems, which showing with the aim of it is protected beside the untrusted server and confidential beside third party verifiers.

4.1 Advantages of Proposed Method

1. Here we stimulate the public auditable scheme of information storage protection in cloud computing and make available a privacy preserving audit protocol. Our system enables exterior auditors to review user's cloud information devoid of knowledge the information contents.

2. The top of our information, our system is the initial to maintain scalable and able auditing mechanism for outsourced cloud storage. specially, our system achieve group audit where several delegate audit tasks from dissimilar user be able to be perform concurrently by the TPA in a privacy preserving approach.

3. Here confirm the protection and validate the show of our future scheme throughout existing experiment and comparison by the "state of the art".

To facilitate Auditing mechanism for outsourced cloud storage below the aforementioned models, our protocol design must accomplish the subsequent protection and presentation assurance:

1. Public audit ability: To consent to Third Party Auditor to authenticate the accuracy of the cloud information ondemand without retrieve a replica of the entire information or introduce added on-line burden to the cloud users.

2. Storage correctness: To make sure that here exists no cheating cloud servers that can pass the check from Third Party Auditor without indeed store user's information intact.

3. Privacy preserving: To make sure that there exists no approach for Third Party Auditor to develop user's information contented from the information collect throughout the Auditing process.

4. Batch auditing: To allow Third Party Auditor with protected and capable auditing capacity to manage with various audit delegation as of probably great amount of dissimilar user concurrently.

5. Lightweight: To allow Third Party Auditor to perform audit with smallest amount communication and calculation overhead.

Algorithm

A public auditing scheme consists of four algorithms " Key Gen", "Sig Gen", "Gen Proof", and "Verify Proof ".

1. **Key Gen**: key generation algorithm that is run by the user to setup the scheme.

RSA involve a *public key* and a *private key.* The public key can be known by each one and is used for encrypting Messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the Private

key. The keys for the RSA algorithm are generating the following way:

Step 1: Choose two distinct prime numbers p and q.

For security purpose, the integer p and q should be chosen at random, and should be of similar bit length.

Prime integers can be efficiently found using a optimality test.

Step 2: Compute $n = pq$. n is used as the modulus for both the public and private keys.

Its length, usually expressed in bits, is the key length.

Step 3: Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function.

Step 4: Choose an digit e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime.

e is release the public key example.

e have a short bit-length and small Hamming weight results in other efficient encryption – most Generally $216 + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in various settings.

Step 5: Determine d as $d \equiv e{-}1 \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$

This is frequently computed using the complete Euclidean algorithm. Using the pseudo code in the

Modular integers section, inputs a and n correspond to e and $\varphi(n)$, respectively is kept as the private key exponent.

2. **Sig Gen**: used by the user to create confirmation metadata, this may consist of MAC, signatures or other information used for auditing.
3. **Gen Proof**: run by the cloud server to generate a proof of data storage correctness.
4. **Verify Proof**: run by the TPA to audit the proof from the cloud server**.**

5. IMPLEMENTATION

The segment of the project when the theoretical proposal is bowed out in to a operational scheme is said to be implementation. So it can regard as to be the most important segment in getting a gainful new scheme in give the operator, guarantee that the recent scheme will job and be competent.

The implementation step includes scheming of process to get different and estimation of different process, thoughtful setup, scrutiny of the accessible system and it's limitation on carrying out.

5.1 Public Audit Ability for Storage Correctness Assurance

To assent to os, the operators who at first downloaded the folder on obscure server, to encircle the capability to confirm the exactness of the downloaded information is in sequence.

Fig4: Data flow from users to Cloud Server

5.2 Operation Support of Dynamic Data

To assent to the operators to carry out wedge stage process on the in order records whereas uphold the parallel level of in order exact assurance. The map must be as able as likely so as to make confident faultless combination shared audibility and energetic information practical support.

5.3 Block less Verification

The confront folder wedge mustn't be recover in the verifier ex.TPA in support procedure used for efficacy distress.

5.4 Dynamic Data Operation with Integrity Assurance

In this demonstrate our system clearly with capably button completely energetic information procedure as well as information alteration (M), information inclusion (I) and information removal for obscure information storage space. In this message that in the successive descriptions, we superior to the folder F also the signature include previously be produce with suitably store in servers. Starting meta data R have been sign by operator with lay up into the obscure servers to others who have the user public key can demanding exactness of information storage space.

Fig5. Dynamic Data Operation with Integrity Assurance

5.5 Data Modification

As we begin starting information changes, which is individual of biggest element commonly used operation in obscure information storages. The fundamental information variation procedure refers to the substitute of literal block with fresh ones. Starting base on the fresh block the user produce the similar signatures. The operators signs the fresh starting meta data R′ by sings (H (R′)) with throw it to server for renew. As a last point, the operator performing the problematic reliability authentication protocol. If the Output is CORRECT, cancel signs (H (R′)), and produce copied folders.

5.6 Batch Auditing for Multi-client Data

During obscure server may at the same time as grip many verification meetings from not equal operators, given K signature on K separate information folder starting K operator, it is extra beneficial to broad all these signature into a lonely small one with validate it one time. To getting this objective, we enlarge our system to allocate for confirmable information

bring up to date and a validation in multi-client systems. The signature system allows the structure of signature on random various messages. In addition, it ropes the aggregation of several signature by not equal signers on dissimilar communication into a exact short signatures, and so appreciably decreases the statement value at the constant time as provided that competent validation for the exactness of all messages.

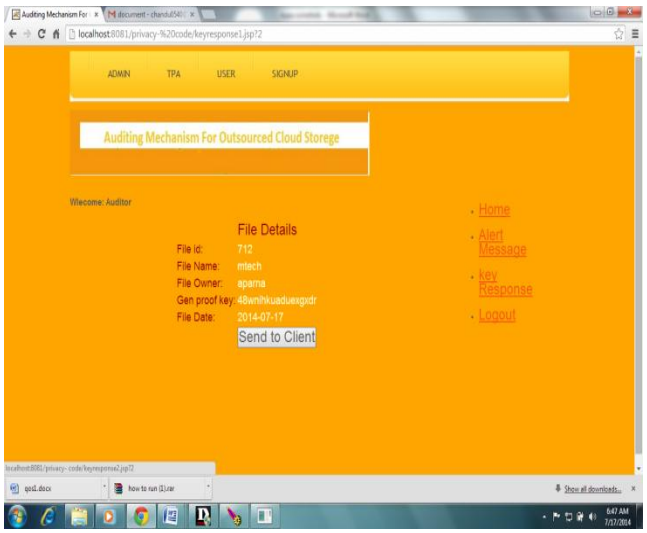
File uploading page

- In this page user can be uploaded data files successfully.

Changing normal data into Meta data

- Here the CS can change the normal data into meta data

Data files sending to TPA page



- Here we can send the file to the TPA for the purpose of cross checking the data.

File downloading page

- Finally the user can download the file when they their data from the cloud.

6. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

Here the prior segment, we contain discuss common set of safety concern useful in public and hybrid clouds. Currently circle our center to some a usual cloud exact security issues. In exact, cloud does find out a set of unique challenge like:
Concept: Cloud's provides a conceptual place of service end-point. For users, it is not possible to pin point in which objective device, storage division (LUN), network port MAC address, switch etc. Actually complex. Thus, in event of security breach, it becomes difficult for a user to separate a particular physical store to have a threats or have be compromise.

6.1 Lack of Effecting Controls

The external cloud's users do not contain fine-gained controls more remote effecting location. Hence the important issues like memory executive, Input calls, right to use to external public utilities and data are remote the preview of the user. Client would want to study the execution traces to ensure that illegal operation are not perform.

6.2 Third-party Control of Data

In clouds, the storage space communications, and thus, the data controls is also with the providers. So constant if the cloud's providers vouches for data confidentiality and integrity, the client may need verifiable proofs for the same.

6.3 Multi-party Processing

In multi-clouds scenario, one party maybe use fraction of the data which further party provide. In lack of strong encryption (as data is individual process), it become essential for participate cloud computing party to protect privacy of individual data.

7. CONCLUSION

Here we intend an Auditing mechanism for outsourced cloud storage. We make use of the homomorphism linear authenticator and random masking to assurance that the Third Party Auditor wouldn't study any information regarding the information content store on the cloud servers throughout the

efficient audit procedure, which not only eliminate the load of cloud users from the tedious and perhaps exclusive auditable tasks, but also alleviate the users fear of their outsourced information outflow. Taking into consideration Third Party Auditor might at the same time as handling various auditing sessions from dissimilar clients for their outsourced information files, we additional expand our Auditing mechanism for outsourced cloud storage into multi user settings, where the Third Party Auditor can execute several audit tasks in a group approach for enhanced effectiveness. Wide-ranging study shows that our scheme is provably protected and extremely competent.

8. FUTUREWORK

We visualize more than a few possible instructions for prospect examine on this region. The mainly capable one we consider is a model in which public verifiability is enforced. Public verifiability, allow TPA to auditing the clouds information storage space without difficult user's time, possibility or funds. An attractive issue in this model is if we can make a system to realize mutually public verifiability and storage truth declaration of dynamic data. In adding, beside with our revise on dynamic cloud data storages, we can also plan to use Trapdoor Commitment system.

9. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[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," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[4] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[5] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Cryptology reprints Archive, Report 2010/234, 2010.

[6] M. Bellare and G. Neven, "Multi-Signatures in the Plain PublicKey Model and a General Forking Lemma,"Proc. ACM Conf.Computer and Comm. Security (CCS),pp. 390-399, 2006.

[7] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols,"Proc. 15th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT),pp. 319-333, 2009.

[8] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession,"Proc. ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.