ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

PRESERVING PRIVACY FOR SHARED DATA ON CLOUD STORAGE SYSTEM WITH SECURITY

Swathi matha P.G,Student,Jyothi.S,Asst professor,Neetha Natesh,Associate professor,DR.AIT,Bangalore

***Abstract*- Cloud computing is effective media for sharing data between different users with low cost efficiency and to take care of cloud users stored data. Providing security and maintain privacy of stored data on cloud storage is another important task for cloud servers. To have identical data and security of stored data is taken care by introducing Third Party Auditing TPA. The Third Party Audit does the work of providing security by creating identical copies of stored data on public cloud to private cloud and also helps in securing privacy by restored data without having complete information on contents of file but will have information on stored file author or file description and track on it. The TPA will main works on by checking the integrity of files on private and public cloud data. TPA is still able to maintain public verification on data which is shared without retrieving whole or complete file but identification of file is unique. TPA uses ring signature to verify correctness of data which is shared. This helps by providing security and privacy for shared data on cloud. Having public and private cloud will leads to have hybrid cloud techniques to maintain security and privacy of shared data on cloud storage.**

***Keywords*— Cloud computing, public auditing, Trusted TPA,security,data Storage,access control.**

I. INTRODUCTION

The paper explains the concepts of more secure hybrid cloud storage on the Amazon's clouds. The existing system will be implemented only public cloud storage, but proposed system something different. The project have so many other advanced concepts also implemented. If we use this proposed system, we will get more secure data from the amazons clouds. Here we are going to use TPA Techniques. The TPA techniques avoids the customer burden of the insecure cloud storage. Now a days many customer after uploading data in amazons cloud, they won't believe for online clouds because so many hackers also there in clouds storages. Because once customer upload data in clouds at the same time TPA send mail for every online user current status of the amazons clouds storage details. If we follow this methods no problems for our future. Here we have three different kind of cloud with us, to maintain the such as well behavior of the cloud performance and capacity in the Amazon's clouds.

Since, user have only offline clouds, because cloud space so much expensive compares to others clouds. That is why we are implemented only offline clouds, but we have some free space gave amazons clouds to access some demo kind of thinks, they newly launch this techniques for only marketing purpose. Now, we do access online and offline this project in WWW application.

II. PROBLEM STATEMENTS

A) Examples Of model:

To analysis the all kind clouds this project to make more secure of the online clouds and offline clouds also. To study about the clouds, how that clouds using in online WWW application and how they make more secure on the clouds, how they avoiding hacker in online, we are going learn this project. Major advantage of this project, to inform every user there cloud storage in online through to email accounts or mobile services. But existing system they don't have this kind techniques, If they want check there cloud should login cloud web site and check, now a days they will SMS or EMAIL alerts. Here main feature to implement for customer secure manor.

That is use of TPA Auditing techniques.,To find the different kind of techniques from here in TPA. Main ethics to secure for privacy preserving data from the amazons cloud on line WWW console web services audit rights to the TPA public and all audits from the TPA are authenticated against such a certificate.

3

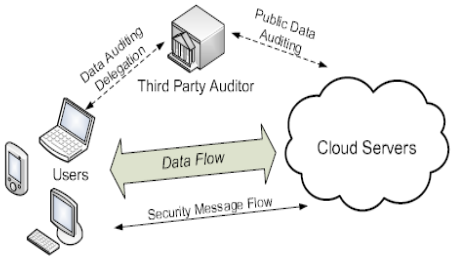

Fig 1. TPA with CSP

(B) Designs:

Secure Privacy-preserving public auditing for cloud Storage paper has above mentioned model, we propose following security and performance Guarantee.

1) *Public auditability*: Allow TPA to verify the Correctness of the cloud data on demand without retrieving a copy of the whole data.

2) *Storage correctness*: Ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users.

3) *Privacy-preserving*: Ensure that there exists no way For TPA to derive users' data content from the information Collected during the auditing process.

4) *Batch auditing*: Enable TPA with secure and efficient auditing capability to efficiency with multiple auditing delegations from possibly large Number of different users simultaneously.

III. PROPOSED SCHEMES

The public auditability is a main drawback of cloud computing technology. In this paper secure public auditing scheme for cloud storage provide more security compared previous technology. In this paper public Auditing system and discuss two straightforward schemes and their demerits. Then we present our main result for privacy preserving Public auditing to achieve the before mentioned design Goals. Finally, we show how to extent our main scheme to batch auditing and encryption algorithms. The batch Auditing used to audit the group of details.

The proposed problem is multi write and problem of TPA if Third-party-auditor not only uses data but also modify the data than how data owner or user will know about this problem. Here the user has two types' keys, one of which only the owner knows called private key and another one which is known to anyone called public key. We match both the data it must be same as the sent one on the sender cannot deny that they sent it . The downloading of data for its integrity verification is not feasible task since it's very costly because of the transmission cost across the network.

1. Public Auditing:

Public auditing scheme algorithms are

1. KeyGen, 2.SigGen, 3.GenProof 4. Verify Proof. *KeyGen* is a key generation algorithm that is run by the user to setup the scheme. *SigGen* is used by the user to generate verification Meta data. *GenProof* is run by the cloud server to generate a proof of data storage correctness. *VerifyProof* is run by the TPA to audit the proof from the cloud server.

2. Batch Auditing*:*

Secure privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple Auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Given *A* auditing delegations on *A* distinct data files from *A* different users, it is more advantageous for TPA to batch these multiple tasks together and audit at one time.

3. Access Control:

Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. The following are six control statements should be consider ensuring proper access control management as in

1. The Access to information.
2. Manage user access rights.
3. Encourage good access practices.
4. Control access to the operating systems.
5. Control access to network services.
6. Control access to applications and systems.

The proposed the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files, as in.

If any two users or more users are using a data, one is writing a data while one is reading a data than it may be wrong read by 1 user, so to resolve data inconsistency is become an important task of the data owner and another problem how to trust on TAP is not calculated. If TPA become intruder and pass information of data or deleting a data than how owner know about this problem are not solved. Integrity and consistency. Proposed scheme in this *virtual machine.*

Advanced Encryption Standard (AES) are used where client encrypt and decrypt the file. In this virtual machine, this mechanism solves the problem of unauthorized access of data. In this suggested scheme that can be used for integrity and consistency of data.

4. Algorithms:

Secure privacy preserving public auditing cloud storage using DES encryption techniques .Rounds and ransformation Stages is an main aspect of this technique. The encryption process executes a round function, Number times, with the number of rounds (Nr) being dependent on key size.

The round function consists of four transformation stages.

1. Sub-Bytes ()
2. Shift Rows ()
3. Mix Columns ()
4. Add Round Key ()

The substitute transformation is an S-Box process that is independent of the key. Each of the bytes of the State is replaced by a different byte, according to a table. The table is fixed and derived from two transformations defined in the standard.The table is an 8 x 8 array, indexed with the State byte. The Shift Rows() transformation is a permutation that is performed row by row on the State array, independently of the key. The first row is not shifted. The 2^{nd} row is circularly shifted left 1 byte. The 3^{rd} row is circularly shifted left 2 bytes.

The 4^{th} row is circularly shifted left 3 bytes. Mix Columns ( ) transformation manipulates each column of the state array.

The process can be described as a matrix multiplication of a polynomial and the state array. This process does not depend on the key. The Add Round Key( ) transformation uses the key schedule word. The process is a bitwise XOR of the columns of the state array, with the key schedule word. Decryption is accomplished using inverses of the transformations, in the appropriate order.

IV. SECURITY ANALYSIS

This section will analyze the Security agreement to confidentiality, integrity the analysis of two aspects.

A. Confidentiality"

The owner of the file is stored on the server before, will use the DES algorithm to Encrypt the data to ensure that the file will not be Intercepted by an unauthorized person to get the file Content. Because encryption and decryption DES uses modular exponentiation, security is Based on the factorization problem, so the factorization Problem is given a composite number N , which is two Large prime numbers p and q the product, if you want Decomposition N , the calculation is not feasible. This also shows if the eavesdropper to intercept the

Cipher text file M though, but because there is no Decomposition of N, it cannot unlock the cipher text file.

B. *Integrity:*

This third party auditor takes care of our data and makes sure that data integrity is maintained. We view the procedure of integrity checking as a key's proficiency within software, platform, and infrastructure security focus area of our cloud architecture. Our vision for helping assure ongoing system integrity in a virtualized environment includes an evolution of integrity checking competences, as in [5] Each phase, in this evolution relies on secure start up enabled and provides an increasing level of assurance and. This evolution begins with one-time integrity checks at system or hypervisor start up, The owner would like to verification cipher text M is a complete file stored on the server at this time, the server will calculate the value of z to prove he has complete store cipher text file M .If the server is calculated z calculated with the owner of the verification value is equal to V , it means the Server does have the correct storage cipher text file M .

Paper Title	Paper Description		
	Description	*Year*	*Author*
			Ravi Kant Sahu
Robust Data Integration While using TPA for Cloud Data Storage Services.	Third party is used to store the encrypted data using AES encryption Algorithm.	2012	Ravi Kant Sahu, Abhishek Mohta and L. K. Awasthi
Third Party Auditing For Secure Data Storage in Cloud Through Digital Signature Using RSA	In this Third party is used to store the encrypted data using private and public key in RSA Algorithm.	2012	Govinda V and Gurunatha prasad H. Sathshkumar
The cloud computing security threats And responses.	Summarize reliability, availability and security issues for cloud computing using access control managements.	2011	Sabahi Farzad

Cloud computing, security is most important task. Cloud computing entrusts services with users data, software and computation on a published application programming Interface over a network. Cloud provides a platform for many types of services. End users access cloud based applications through a web browser or a light weight desktop or a mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give same or better service and performance than if the software programs were installed. cloud Security, maintaining data integrity is one of the most important and difficult task. When we talk about cloud users, they are using cloud services provided by the cloud provider and again, in the case of maintaining integrity of the data, so we cannot trust the service provider to handle the data, as he himself can modify the original data and the integrity may be lost. If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider. So, in this case, we take the help of a trusted third party auditor to check for the integrity of our data. This third party auditor takes care of our data and makes sure that data integrity is maintained.

V.IMPLEMENTATION

In the paper, to find the more security of the cloud and more real time oriented task also, we can handles based on the internet clouds like drop box etc..To make double authentication based on image layers and limited of cloud service provider (CSP).Centralizated service provider based on the EM2 Web service on the live. To share any important data from the one server into another server based on the KDC Symmetrically methods.But, existing system they have so many other cloud service also. Proposed system we are going to use different ways of cipertext techniques based on the RTOS CLOUDS.

5.1 USER

To create new account for no. of user to check our data security in decentralizated techniques based on the cloud storages.Not a limited user, we create number of user based the your systems securitiesUser created based on the location, because to find out user, which area they created account, otherwise we are getting confusion.After create account, we should login for entire account from the cloud server from the amazons servers.Our record store to amazons cloud for double authentication purposes.Finally login for user to see out main web pages. But ,If we use TPA Techniques, user will get lifelong secure from internet storage out in very safe for amazons clouds.

5.2 OWNER

To create new account for no. of OWNER to check our data security in decentralizated techniques based on the cloud storages.Not a limited OWNER, we create number of user based the your systems securitiesUser created based on the location, because to find out user, which area they created account, otherwise we are getting confusion.After create account, we should login for entire account from the cloud server from the amazons servers.Our record store to amazons cloud for double authentication purposes.Login for both account user and owner.

5.3 TPA AUDITING

To check whether they have same data already upload or not, if upload same data they will show some ALERTS message otherwise they won't show anything means yours documents approved.
Its supports any kind of documents format to upload in cloud location and in the cloud unlimited storage look like amazons.There are two type documents securities there Check documents TPA Authentication privacy.SMTP interface end point.Check ,if any document missing or not If missing immediately sending all user some SMS OR MAIL ALERTS.This is not particular user; they will send the entire user, who ever create account with TPA Integrity.Here showing date, time and which document we are upload in the clouds everything display on the JSP TABLES.If any modification happen in the TPA location, their will get complete EMAIL ALERT message from the amazons clouds.This is main purpose of project in privacy preserving clouds.

VI.CONCLUSION

It's a system of providing security where the system is online, so it can be improved further and hosted Mobile Apps.The security is limited, so some additional security measures could be made to provide more security to the system.There is no provision of complain handling, so further it can be added.The whole system can be automated so that the whole Storage process requires minimal human intervention This is platform independent.To support multiple language like c#,j# and pythons also.Try to access free licenses on the Amazon cloud in future aim for 2016 base paper.To implement future plan in Big Data in Cloud Optimization.

REFERENCES

[1] Q.Wang ,C.Wang, j.Li, K.Ren, and W.lou, "Enabling public verifiability and data dynamics for storage security in cloud computing".

[2] H.shacham and b.waters "compact proofs of retrivability "in proc. Of asiascrypt 2008.

[3] P.Mell and T,Grance, "Draft NIST working definition of cloud computing", referred on june 3rd 2009.

[4] M.AShah,R.Swaminathan, and M.Baker"privacy-preserving audit and extraction of digital contents".

[5] Armbrust, A.Fox, R.Griffith, A.D.Joseph, and M.Zaharia,"Above the clouds:A Berkeley view of cloudcomputing", feb 2009

[6] M.A.Shah, M.Baker, J.C.Mogul, and R.swaminathan, "Auditing to keep online storageservices honest", in Proc.of hotOS'07.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud

Computing," Proc. 14th European Symp. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[8] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[9] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, Oct. 2007.

[10] 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 Distributed Systems, vol. 22, no. 5,pp. 847-859, May 2011.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEEINFOCOM, pp. 525-533, 2010.

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

[13] K. Yang and X. Jia, "Data Storage Auditing Service in CloudComputing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.

[14] Q. Wang et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS '09, Sept.2009, pp. 355–70.