ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Secure Privacy Preserving Public Auditing for Cloud storage

Sathiskumar R[1], Dr.Jeberson Retnaraj[2]

Department of Information Technology, Sathyabama University, Chennai, India[1]

Department of Information Technology, Sathyabama University, Chennai, India[2]

Abstract— Cloud storage provides users to easily store their data and enjoy the good quality cloud applications need not install in local hardware and software system. So benefits are clear, such a service is also gives users' physical control of their outsourced data, which provides control over security problems towards the correctness of the storage data in the cloud. In order to do this new problem and further achieve secure and dependable cloud storage services. The main goal of cloud computing concept is to secure, protect the data and the processes which come under the property of users. The security of cloud computing environment is an exclusive research area which requires further development from both the academic and research communities. In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper we proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced data in cloud Environments.

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

I. INTRODUCTION

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. Storing data into the cloud offers great help to users since they don't have to care about the problems of hardware problems. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is avoids the responsibility of local machines for data maintenance at the same time. As a result, users are at the interest of their cloud service providers for the availability and integrity of their data the one hand; although the cloud services are much more powerful and reliable than personal computing devices and broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time. On the other hand, since users may not keep a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Our work is among the first few ones in this field to consider distributed data storage security in Cloud Computing.

II. PROBLEM STATEMENTS

A) Examples Of model:

The *cloud user* (U), Large amount of data files to be stored in the cloud. The *cloud server* (CS), which is managed by *cloud Service provider* (CSP) to provide data storage service and Storage space and computation resources .The *third party Auditor* (TPA), cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. The dynamically interact with the CS to Access and update their stored data for various applications Purposes. Users may resort to TPA for ensuring the Storage security of their outsourced data, while hoping to keep Their data private from TPA. The TPA, is in the business of auditing, is reliable and independent, and thus has no incentive to the CS or the users during the auditing process. cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. Any possible leakage of user's outsourcing data towards TPA through the auditing protocol should be prohibited. The TPA's audits, the user can sign a certificate granting audit rights to the TPA's public key,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

and all audits from the TPA are authenticated against such a certificate.

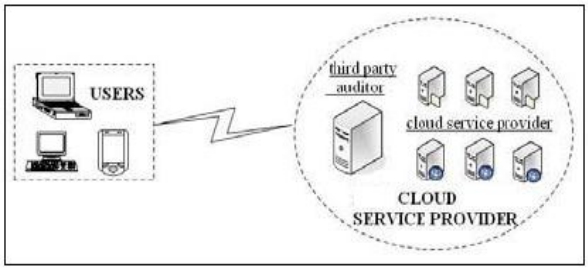

Fig 1. TPA with CSP

(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.*

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

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 2nd row is circularly shifted left 1 byte. The 3rd row is circularly shifted left 2 bytes. The 4th 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 .

Usecase Diagram

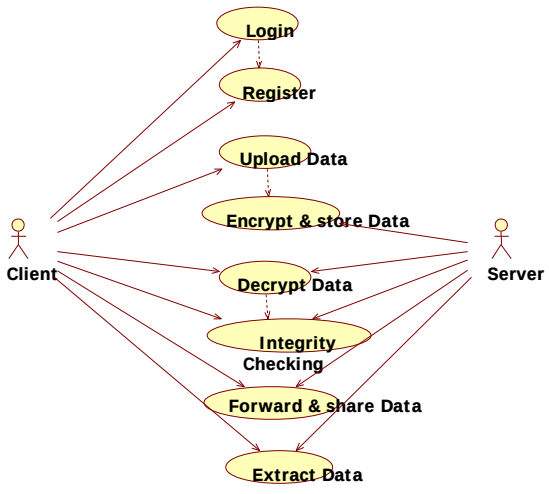

TABLE I. SIMILIER PAPER AND DETAIL DESCRIPTION

Paper Title	Paper Description		
	Description	*Year*	*Author*
Using third party auditor for cloud security	Third party Auditor is used to store the data in cloud with more security.	2013	Ashish Bhagat

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

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. CONCLUSION

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 paper provides an abstract 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 and client.

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.

[15] C. Erway et al., "Dynamic Provable Data Possession," Proc. ACMCCS '09, Nov. 2009, pp. 213–222.

[16] C. Wang et al., "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar.2010.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

[17] Cong Wang and Kui Ren, Illinois Institute of Technology WenjingLou, Worcester Polytechnic Institute Jin Li, Illinois Institute of Technology "Toward Publicly Auditable Secure Cloud Data Storage Services". 0890-8044/10/2010 IEEE.