N.Lavanya *et al*, International Journal of Computer Science and Mobile Applications,

Vol.2 Issue. 4, April- 2014, pg. 77-81 **ISSN: 2321-8363**

EFFICIENT THIRD PARTY AUDITING IN SECURE CLOUD

N.Lavanya[1], R.Mythili[2]
[1]M.Tech (Computer science and Engineering) (final year), SRM University
[2]Assistant Professor, SRM University

ABSTRACT

In this paper we talk about the evolvement of cloud computing model and there a structure for secure cloud computing through third party auditing. The giving of the paper is to understand the suggestion of cloud computing and what is meant secure cloud computing via third party auditing rather than suggest a new style and new knowledge to secure cloud computing. Our holistic advance has planned value to those who are using or think using cloud computing because it addresses concerns such as security, privacy and regulations and compliance. In this object, we focus on cloud data storage security, which has always been an important aspect of quality of service. Including: data update, delete and append. Security and performance analysis shows that the proposed scheme is highly efficient and resilient against complex crash, mean data change attack, and even server colluding attacks.

Keywords: Cloud Security(CS), Cloud service provider(CSP), Third party auditor(TPA), Cloud Computing

1. INTRODUCTION

Cloud computing is a method in which computing power, memory, infrastructure can be delivered as a service. A Cloud computing is a set of network enabled services, guaranteed QoS, inexpensive computing infrastructures on demand with an easy and simple access. Cloud computing is a model which enables convenient, efficient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud security is an evolving sub-domain of computer security, network and information security. Security in cloud can be implemented remotely by client where the data centers and protocols in the security objectives of the service provider are: i) confidentiality for securing the data access and transfer ii) auditability for checking whether the security aspect of applications has been tampered or not. Dimensions of cloud security have been aggregated into three areas like security and privacy, compliance and legal issues.

2. CLOUD SERVICES

A. ***Cloud software as a service (SaaS):*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The application is accessible from various client devices through web browser.

B. ***Cloud platform as a service (PaaS):*** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application created using programming languages and tools supported by the provider. operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

C. ***Infrastructure as a Service (IaaS):*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

D. ***Deployment Models in Cloud computing:***

There are four types of cloud available in cloud computing i.e. private cloud, public cloud, hybrid cloud and community cloud as shown in Fig 1. These deployment models describe who owns, manages and is responsible for the services.

3. THIRD PARTY AUDITOR

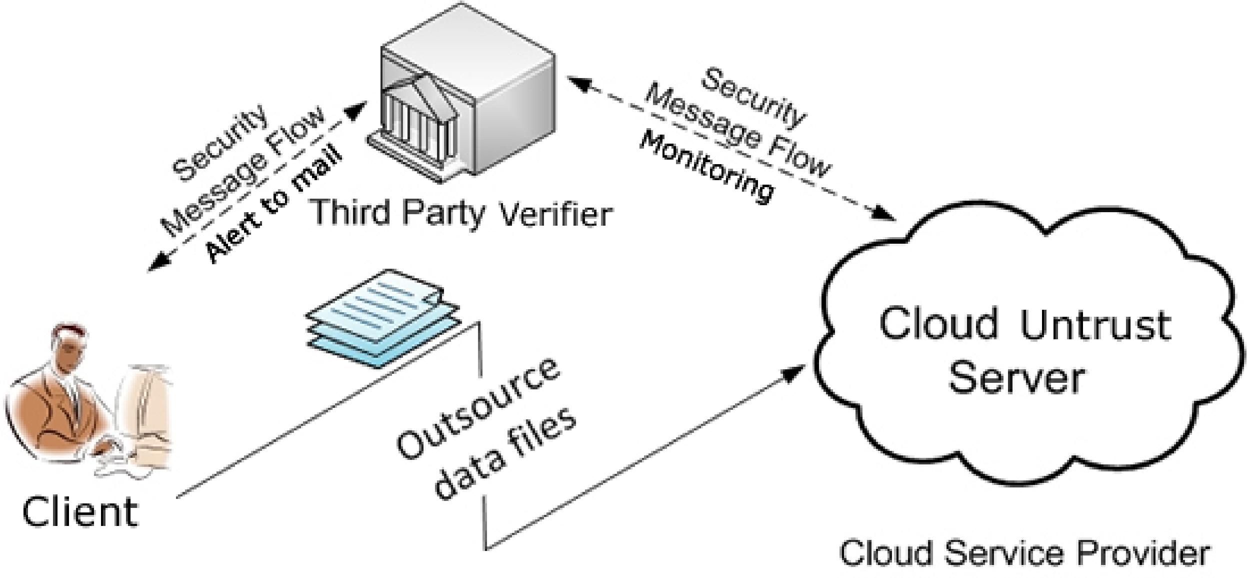
Third Party Auditor is type of checker. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

4. EXISTING SYSTEM

To introduce an efficient TPA for both security and privacy of cloud data. It should met some fundamental requirements: the cloud data must be audit by the TPA without demanding local copy of data and reducing the online burden of the users. The TPA caused due to various auditing protocols like public auditing, privacy preserving public auditing. In the existing model, provides a secure TPA based storage utilizing homomorphic token and distributed erasure coded data which allows users to audit the cloud storage with very light weight communication and computation cost. The auditing results in strong cloud storage correctness guarantee and fast data error localization.

5. PROPOSED SYSTEM

TPA ensures the accuracy of data and allows the cloud client, to verify the honesty of the data stored in the cloud. The outflow of the user's outsourced data from the auditing protocol makes security and honesty problems in the cloud. Security to the TPA should provided by using agreement protocol for key generation. By using the agreement protocol, session id will be generated between TPA and server .these keys are used to connect the server and TPA . Based on this session key, client can receive the file from the server.



6. RELATED WORK

STORAGE SECURITY AND PUBLIC AUDITABILITY

Users rely on the cloud server (CS) for cloud data storage and maintenance. They may interact with the CS to access and update their stored data for various applications. The Third Party Auditor (TPA) eliminates the auditing of client to check where his data is stored in the cloud. Since the services in cloud computing are not limited to data backup ,so the dynamic support of data such as block modification, insertion and deletion is significant . The previous works lacks the support of either public auditability or dynamic data operations, where it achieves the both with remote data integrity.

It first identifies the security problems and difficulties of direct extensions with full dynamic data updates from the prior works and then shows how to construct a verification scheme for the integration. By manipulating the classic Merkle Hash Tree construction for block tag authentication the efficiency of data dynamics can be achieved. To support efficient handling of multiple auditing tasks, the technique of bilinear aggregate signature to extend the result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

PRIVACY-PRESERVING PUBLIC AUDITING

The Security problems in cloud computing creates the burden to the local data storage and maintenance. By utilizing public auditability the users can resort to an external audit party to the integrity of outsourced data when needed.

The auditing process by the TPA should not bring any new vulnerabilities towards user data privacy and should not increase the burden of the user .To overcome these disadvantages and to introduce a secure cloud storage with a auditing .The main task is to guarantee that the TPA should not learn any knowledge about the content of data stored on cloud server during the auditing process, can be achieved by using the homomorphic non-linear authenticator and random masking. A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof). 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 metadata, which may consist of digital signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof. Running a public auditing system consists of two phases, Setup and Audit:

Setup: The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and deletes its local copy. As part of preprocessing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof. By using privacy preserving public auditing should achieve the following design goals:

Public audit: The correctness of the cloud data can be verified by the TPA without retrieving the copy of the data.

Storage Consistency: The data, which is in the cloud server, will pass the audit from TPA without storing it.

Privacy preserving: It must guarantee that there is no way to get user's data content from the collected information.

Batch auditing: Provide TPA with secure and efficient auditing ability with multiple auditing delegations.

DATA DYNAMICS

In cloud storage users will no longer posses the local copy of the outsourced data after storing the data. So the client should verify the integrity of the data stored in the remote entrusted server. To overcome these problems a remote integrity checking protocol. This protocol is suitable for providing integrity protection of cloud data. It also supports data insertion, modification, and deletion at the block level with the support of public verifiability.

Public verifiability provides client to verify the integrity task to TPA while they themselves can be unreliable or not able to commit necessary computation resources with continuous verifications. It is proved to secure against an untrusted server and private against third party verifiers.

SECURE AND DEPENDABLE STORAGE SERVICE

The physical possession of the outsourced data creates new security risks in the cloud computing storage. This paper provides a secure TPA based storage utilizing homomorphic token and distributed erasure coded data which allows users to audit the cloud storage with very light weight communication and computation cost. The auditing results in strong cloud storage correctness guarantee and fast data error localization.

To ensure the dynamic nature of the cloud data, the proposed design supports secure and efficient dynamic operations on outsourced data including block modification, deletion and append. The analysis shows the efficiency and resilient against Byzantine failure, malicious data modification attack and server colluding attacks.

To provide redundancy parity vectors and guarantees data dependability using erasure-correcting code in the file distribution preparation. Utilizing the homomorphic token and distributed verification of erasure coded data helps to achieve the integration of storage correctness insurance and data error localization. The advantages of dynamic data verification are

Storage correctness: Ensuring the user's data are stored appropriately and kept intact all the time in the cloud.

Fast localization of data error: Malfunctioned server can be easily located during data correction.

Dynamic data support: The same level of storage correctness assurance during user's modification, deletion or append the data files in the cloud should be maintained.

Dependability: Enhance data availability against Byzantine failures, malicious data modification and server colluding attacks.

Light weight: Perform storage correctness checking's with minimum overhead

BATCH AUDITING

With the organization of privacy-preserving public auditing, the TPA may simultaneously handle multiple auditing upon different users' allocation. The entity auditing of these tasks for the TPA can be tedious and very inefficient. Given K auditing delegations on K distinct data files from K different users, it is more advantageous for the TPA to batch these multiple tasks together and audit at one time.

CONCLUSION

Cloud computing security has brought us with great challenge. Security in cloud computing can be accessed with TPA and without TPA. In the cloud computing by using the TPA method, we can increase the data security which is basically a circulated storage system. To ensure each data access in control and reduce the difficulty of cloud computing by help of Advance Encryption Technique (AES).Session Key techniques are used to provide secure communication between the client and the cloud. The system ensures that the client's data is stored only on trusted storage servers and it cannot be transferred by malicious system administrators to some corrupt node. Symmetric key sharing is handled with public key cryptography, to achieve faster performance and low computational overhead. The system achieves confidentiality and integrity of the client's data stored in the cloud. Also secure and efficient data dynamic operations such as update delete and append on the data blocks stored in the cloud. Our future goal is to design a secure cloud storage system with TPA which addresses the issues mentioned.

REFERENCES

[1] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609

[2]. Ateniese G, Pietro R.D, Mancini L.V, and Tsudik G, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New York, NY, USA: ACM, 2008, pp.1-10.

[3] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, andP. Rogaway. UMAC: Fast and secure message authentication.In *CRYPTO*, volume 1666 of *LNCS*, pages 216–233, 1999.

[4] Bowers K.D, Juels A, and Oprea A, "Hail: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009, pp. 187–198.

[5] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461, 2002

[6] Chang E.C, and Xu J, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

[7] Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," *in Proceedings of Natural Sciences and Engineering*, Sweden, pp. 2-4, 2010.

[8] Cong Wang,Qian Wang,Kui Ren Ninig Cao and Wenjing Lou"Towards Secure and Dependable storage services in cloud computing",IEEE Transaction on service computing,vol 5,no 2,june 2012

[9] Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011

[10] Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012

[11] Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012

[12] Metri P. and Sarote G., "Privacy Issues and Challenges in Cloud computing," *International Journal of Advanced Engineering Sciences and Technologies*, vol. 5, no. 1, pp. 5-6, 2011.

[13] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012

[14] D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011

[15] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing tokeep online storage services honest," in *Proc. Of HotOS'07.*, CA, USA: USENIX Association, 2007, pp. 1–6.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS '09), pp. 1-9, July 2009