ISSN:0975-9646

"Providing Security And Privacy To Cloud Data Storage"

Yogesh V. Bhapkar, Rakesh S. Gaikwad, Milind R. Hegade
ISB&M, SOT, PUNE, SPPU PUNE,
MAHARASHTRA , INDIA

***Abstract*— Cloud Computing is the next generation of Information Technology. Using Cloud Computing we can access remote data, we can purchase storage space, we can develop application software etc. The security related to cloud data storage is main concern. To provide security to cloud data storage we are implementing such a system that not only provide security but also maintain privacy between Third party auditor And Cloud service provider.**

***Keywords*— Cloud Service provider, Third Party Auditor, AES, SHA-1, Attacker Module.**

I.INTRODUCTION

Cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications. Cloud storage system enables storing of data in the cloud server efficiently and makes user to work with the data without any trouble of the resources. Cloud Computing is evolving and considered next generation architecture for computing.

The client store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. In cloud computing, since the data is stored anywhere across the globe, the client organization has less control over the stored data. To built the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access A trusted 3rd party cloud provider be used to provide security services, while the other cloud provider would be data storage provider. Service provider would not store any data at its end, and its only confined to providing security service.

The application or software will provide data integrity verification by using hashing algorithm like SHA-1 and provide encryption/decryption using symmetric algorithm like AES, and defining band of people who can access the shared data securely can be achieved by defining access list. The Software is only responsible for encryption /decryption, computing/verifying the hash of the data and does not store any data in trusted 3rd party security system server. The encrypted data along and original data hash are stored in Separate Cloud (Security Cloud), therefore even if the storage cloud Privacy Preserving Public Auditing For Secure Cloud Storage system administrator has access user data, since the data is encrypted it will be difficult for the system administrator to understand the encrypted data. While the user down-loads the data from Storage Cloud, it is decrypted first and then new hash is calculated which is then compared with hash of original data stored in Security Cloud.

Finally, this software/application provides the user with the ability to store the encrypted data in Storage cloud and hash and encryption/decryption keys in security cloud service, and no single cloud service provider has access to both. Other benefit of delegating responsibility to trusted 3rd party is that it reliefs the client from any kind of key management or over head is maintenance of any key information related to data on it device, because of which it allows the client to use any browser enabled devices to access such service.

A) Public cloud

Public clouds are clouds that are run by third-party service providers. in this deployment model, various types of applications from different customers are likely to be hosted together, on the same cloud infrastructure. Public clouds are open to the consumers but the cloud service provider has the full ownership with its own policy.

B) Private cloud

A private cloud built exclusively for use by one organization. In this model the organization itself owns the cloud and has full control of deployment and application use.

C) Hybrid cloud

It is usually combination of public and private cloud. Organizations use the hybrid cloud model to optimally utilize in-house resources.

Cloud computing service models

A) Software as a service

It is a software delivery model in which applications are hosted by a service provider and make available to customers over a network.

B) Platform as a service

It is a development platform provided as a service which supports the full software life cycle. It allows users to develop cloud based services and applications.

C) Infrastructure as a service

It is a cloud service model that provides basic data storage and computing capabilities as standardized services over the network.

Security issues in cloud

Every coin has two sides. There is criticism about privacy in cloud model, a administrator have access to data stored in the cloud. They can access the client data. Traditional security and protection techniques need a for cloud. Except for private cloud where organization does not have control over the equipment, the progress of cloud seems little slow, because organization thinks instead of compromising on the security of the data, they are still willing to invest in buying private equipment to setup there own infrastructure. Security issues which are of concern to the client can be classified into sensitive data access, data segregation, bug exploitation , recovery , accountability, malicious insiders, account control issues. Like cryptography , use of more than one cloud provider, strong service agreement between client and cloud service provider. heavy investment is needed to secure the compromising data in cloud . cloud can be grow only if it is possible to build in client and server.

II.LITERATURE SURVEY

This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, they consider the task of allowing a third party auditor to verify the integrity of the dynamic data stored in the cloud. [3]

In this paper, they proposed an effective and flexible distributed scheme with dynamic data support to ensure the correctness of cloud data. [11]

Advantages:

1. Using the homomorphic token with distributed verification of erasure coded data, this system achieves the integration of storage correctness insurance and data error localization.
2. This system is highly efficient.
3. Malicious data attack and server colluding attacks.
4. This system guarantees the data dependability.

Limitations:

1. This system provides less security as compared to the system in which encryption/decryption algorithms are used.
2. This system is inconvenient.
3. This system does not provide data recovery

III.PROPOSED SYSTEM

The proposed system is an effective and flexible distributed Scheme with explicit dynamic data support to to ensure the correctness of users data in the cloud. To fully ensure the data integrity and save the cloud users computation it is of critical importance to enable public auditing service for cloud data storage, so that users may depend on independent third party auditor to audit the outsourced data. The Third party auditor can periodically check the integrity of all the data stored in the cloud .which provides easier way for the users to ensure their storage correctness in the cloud.

Goals

The goal of our project is to provide the security for the data that are stored in the cloud and to increase the security level& to securely introduce an effective TPA .

Objective

Our objective is to build a security service which will be provided with a trusted 3rd party, and would lead to providing only security services and wouldn't store any data in its system.

1. To construct Web service system which would provide data integrity verification, provide encryption/decryption of the consumer data
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this web service before uploading /downloading the data to and from cloud.

Scope

To support scalable and efficient privacy-preserving public storage auditing in cloud. The mechanism on commercial public cloud as an important future extension.

System Features

1. Batch Auditing: To enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

2. Public auditability: To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

3. Privacy preserving: To ensure that the TPA cannot derive user’s data content from the information collected during the auditing process.

Advantages

1. Lightweight: TPA perform auditing with minimum communication and computation overhead.
2. Storage correctness: To ensure that there exists no cheating cloud server that can pass the TPAs audit without indeed storing users data intact.
3. Our scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud.
4. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy preserving manner.

Disadvantages

1. Internet-facing Services

The cloud service which is accessed over the internet via browser, the quality of service delivered on the network is another concern

2. System Complexity: All these components and interaction of these components with each other needs to be addressed.

Applications

1. Government section or our system make as a legal organization who audits users data.
2. Corporate industry.
3. for cloud data security

IV. System Architecture

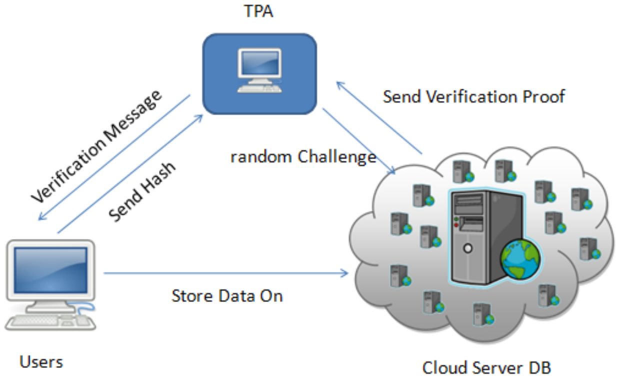

Figure1:Physical Structure of a System

Modules

1.user

A user which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.

2. Cloud storage server

It is is managed by Cloud Service Provider, has significant storage space and computation resource to maintain the client data.

3. Third party auditor

It is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

The data owner registered with cloud service provider and stores their data in cloud server by using the private key. To check the integrity of data stored in cloud server, user sends request to Third Party Auditor. The TPA audit the files stored in cloud server by using top hash value which it get from the data owner. Running a public auditing system consists of two phases,

Setup:

The user initializes the public and secret keys using AES algorithm and then calculate the hash of the file and send it to the third party auditor.

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 gives the response message .TPA verify the hash and maintains the log. If something happen wrong related to data then TPA send message to the Client.

4. Attacker module

The attacker module is used for breaking security of a cloud data storage.

V. Conclusion

In cloud computing the Third Party Auditor guarantee that the cloud service provider & also itself TPA would not learn any knowledge about the data that is stored on the cloud server. During the efficient auditing process, it not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task. The partitioning of data will enables storing of the data in easy and effective manner. It also gives way for flexible access and there is less cost in data storage. The space and time will also effectively reduce during storage. Also the remote data integrity checking detects the threats and misbehaving server while storing the data in cloud ensuring data security. Calculating digital signature may secure file more efficiently.

References

[1] http:en.wikipedia.org/wiki/SHA1

[2] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.AtanuRakshit, "Cloud SecurityIssues", IEEE International Conference on Services Computing, pp. 517-520,September 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",IEEETrans Parallel and Distributed Systems, May 2011.

[4] Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE,"Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE TRANSACTIONS ON COMPUTERS, 2013.

[5] William Stallings, "Cryptography and Network Security", 2009.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song ,"Provable Data Possession at UntrustedStores", Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 598-609, 2007.

[7] M.A.Shah,M.Baker,J.C.Mogul,and R.swaminathan, "Auditing to keep online storage services honest", in Proc.of hotOS07.

[8] 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

[9] Peter Mell, Timothy Grance, "The NIST Defnition of Cloud Computing", NIST Special Publication 800-145

[10] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal In- formation Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.

[11] Cong Wang, Qian Wang, Kui Ren And Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing”, in IEEE 2010.

[12] C.Selvakumar,G.JeevaRathanam,M. R. Sumalatha, “Improving Cloud Data Storage Security Using Data Partitioning Technique”, in IEEE 2012.