Survey on Secure and Data Dynamics Storage in Cloud Computing

Manasi Doshi
PG student of Department of
Computer Engineering,SCOE,
Pune,India

Swapnaja Hiray
Associate Professor of Department of
Computer Engineering,SCOE,
Pune,India

Abstract

Cloud computing is the use of computing of sources that are delivered as a service over a network. Cloud enables users to store their data, but data is stored at remote location. A major characteristic of the cloud services is that user's data are usually processed remotely in unknown machines that users do not operate. So, basic need is to provide security to cloud server. One of the most challenging problem in Cloud computing is about the security of the outsourced data which is mainly handled by untrusted parties. Another reason for doing independent literature survey of this is simultaneous comparison of different papers and to identify the future research areas and methods for improving the existing drawbacks.

IJERT

1. Introduction

In cloud computing we can share our data and application at common place. This uses internet and share resources to provide services. Security is important issue because cloud having many benefits so, it have many users and data is remotely located. Various attacks can hamper to original data and may misuse confidential data. This paper focuses towards security to cloud. This contains multiple ways of providing security to cloud data.

2. Related Work

In this section we first review related works addressing security in cloud. Security issue is very important in cloud there are many techniques available so here is review of all these.

Data security is the major challenge in the cloud computing as user's data reside in the servers which are remotely situated and far away from the end-users. These data may include confidential data (financial data, health records), personal information which may be disclosed to competitors or publicly. So security emerges as the highest priority issue [2]. In [3] Third party auditor for verification, they describes three network entities i.e. client which is user, cloud storage server which is handled by cloud service provider and Third party auditor which is verifier.TPA having public key, it is act with only trusted server, they are not focuses on data privacy. In [4] it defines 2 basic schemes. Scheme 1 : User computes the MAC of every file block. Transfers the file blocks & codes to cloud and shares the key with TPA. During the Audit phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding MACs to verify the correctness of the data file. Drawback of this scheme is TPA can see cloud data. Scheme 2: In Setup phase, User uses s keys and computes the MAC for blocks and user shares the keys and MACs with TPA. During Audit, TPA gives a key (one of the s keys) to CSP and requests MACs for the blocks. TPA compares with the MACs at the TPA. Improvement from Scheme 1: TPA doesn't see the data, preserves privacy. Drawback: a key can be used once, Schemes 1 & 2 are good for static data (data doesn't change at the cloud). In paper [5] they discuss main challenges for achieving cloud computing services, this problem focuses on accountability in cloud computing. Accountability means verification of access control policies. In their subsequent work [6], propose a dynamic version of the prior PDP scheme. the system does not support fully dynamic data operations, i.e., it only allows very basic block operations with limited functionality, and block insertions cannot be supported.

3. Reqiurements of security to cloud

3.1 Principles of information security

1. Confidentiality

It refers to prevention of intentional and unintentional unauthorized access to information. Confidentiality in cloud systems related to areas of traffic analysis, encryption and inference.

To ensure confidentiality use:

- Network security protocol
- Network authentication services
- Data encryption services

2. Integrity

It refers to consistency of actions, values, methods, measures, principles, expectations and outcomes. Cloud information integrity requires following 2 principles to meet modifications are not made to data by unauthorized person and unauthorized modifications are not made to data by authorized person.

To ensure integrity use:

- Firewall services
- Communication security management
- Intrusion detection services 1

3. Availability

It ensures the reliable and timely access to cloud data or cloud computing resources by appropriate person. It guarantees that the systems are functioning properly when needed and guarantees that security services of cloud system are in working order.

To ensure availability use:

- Fault tolerance for data availability, such as backups and redundant disk system
- Acceptable logins and operating process performance

IJERT IJERT

3.2 Cloud Security Services

Factors that affect cloud software assurance include:

1. Authentication

It is a one way to confirm the identity of person of program. Authentication often involves verifying the validity of at least one form of identification.

2. Authorization

It refers to specifying access rights to individual that enable access to computer resources and information.

3. Auditing

To maintain operational assurance, organizations use 2 basic methods: system audits and monitoring. These methods can be employed by the cloud customer, cloud provider or both. A system audit is a one time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or users such as intrusion detection.

4. Accountability

It is ability to determine the action and behaviours of a single individual within the cloud system and to identify that particular individual. Audit trails and logs support accountability.

3.3 Cloud entities

There are some entities that are commonly used in cloud client, Third Party Auditor (TPA), Cloud Service Provider (CSP), Cloud Server (CS).

1. Client:

   Client is that entity who is using of cloud services and who has to store data on cloud. Multiple clients can use cloud storage services.

2. TPA:

   TPA is an optional entity. It has expertise and capability to expose dummy client. E.g. authentication of client.

3. CSP:

   CSP is an entity which provides cloud services. E.g. client want to upload file then CSP give call to CS.

4. CS:

   CS is an entity which allow client to perform operation on data stored on it.

4. Storage techniques in cloud computing

4.1 Secure and Dependable Storage Services in Cloud

It is based on distributed storage on particular no. of machines. It uses homomorphic token for checking integrity of data. This helps user low cost communication and computational cost. The auditing result ensures strong cloud storage correctness as well as simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. It allows client to perform secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

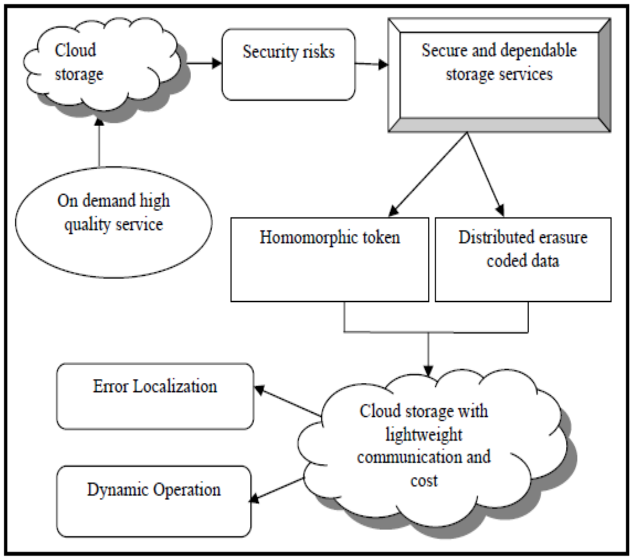
Cloud storage
Security risks
Secure and dependable storage services
On demand high quality service
Homomorphic token
Distributed erasure coded data
Error Localization
Cloud storage with lightweight communication and cost
Dynamic Operation

Figure 1. Secure and Dependable Storage Architecture

4.2 Privacy Preserving Public Auditing for Secure Cloud Storage

It consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof)

- KeyGen:

It is run by the user to generate public and private parameters.

- SigGen:

It used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing

- GenProof:

It is run by the cloud server to generate a proof of data storage correctness

- VerifyProof:

It is run by the TPA to audit the proof from the cloud server.

IJERT

Our public auditing system can be constructed from the above auditing scheme in two phases, Setup and Audit:

1. Setup:

   The user generates the public and secret parameters of the system by executing KeyGen, and pre-processes the data file F by using SigGen to generate the verification metadata. The user then stores the data file F at the cloud server, delete its local copy, and publish the verification metadata to TPA for later audit. As part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

2. 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 from a function of the stored data file F by executing GenProof. Using the verification metadata, the TPA verifies the response via VerifyProof.

Basic Scheme I:

User computes the MAC of every file block. Transfers the file blocks & codes to cloud, shares the key with TPA. During the Audit phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding MACs to verify the correctness of the data file. Drawback: TPA can see cloud data.

Basic Scheme II:

In Setup phase, User uses s keys and computes the MAC for blocks and user shares the keys and MACs with TPA. During Audit, TPA gives a key (one of the s keys) to CSP and requests MACs for the blocks. TPA compares with the MACs at the TPA. Improvement from Scheme 1: TPA doesn’t see the data, preserves privacy.
Drawback: a key can be used once, Schemes 1 & 2 are good for static data (data doesn’t change at the cloud)

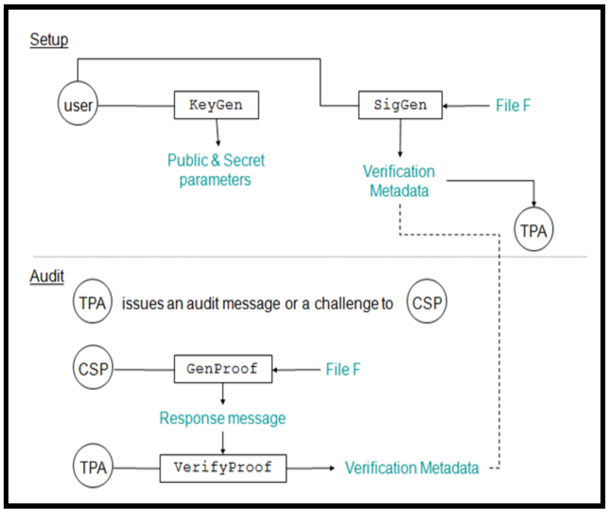

Figure 2. Public Auditing Storage Architecture

4.3 Public Auditability and Data Dynamics for Storage Security in Cloud

Public auditing system with protocol that supports complete dynamic data operations is presented [7]. To accomplish dynamic data support, the existent proofread of PDP or PoR scheme is improved by spoofing the basic Markle Hash Tree (MHT) for block tag authentication. Proposed system extended in the direction of allowing TPA to perform many auditing jobs by examining the bilinear aggregate signature technique. It performs blockless verification.

IJERT

Table 1. Comparative analysis of existing storage techniques

Storage Scheme	**Proposed Approach**	**Advantages**	**Restrictions**
Implicit Storage Security to Online data[10]	Data partitioning scheme for online data storage	Partitioned data pieces cannot bring out any user information	In case user forgot where the data stored, it will become difficult for users
Identity-Based Authentication[11]	New authentication protocol based on identity which is based on hierarchical model	Weightless and more expeditious	Only certificate communication is taken into account.
Efficient Third Party Auditing (TPA)[12]	Novel and uniform security structure. Storage security is accomplished by utilizing BLS algorithm	Auditor performs auditing jobs for different users at the same	Unable to support both public verification and dynamic data correctness
Effective and Secure Storage Protocol[13]	Efficient and secure storage protocol is implemented by utilizing Elliptic curve cryptography and Sobol Sequence	Block level data dynamic operations are also used to maintain the same security assurance	Elliptic Curve Cryptography scheme is only suitable for devices with restricted low power

5. Conclusion

Cloud Computing is an emerging computing paradigm, allows users to share resources and information from a pool of distributed computing as a service over Internet. Even though Cloud provides benefits to users, security and privacy of stored data in cloud are still major issues in cloud storage.In this paper, the different mechanisms presented by different authors are analyzed. Finally, presented a comparative analysis on storage techniques, that includes the proposed approach, advantages and limitations of those storage techniques.

References

[1] C. Wang, Q. Wang, K. Ren, N. Cao, W.Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE transactions on services computing, VOL. 5, NO. 2, APRIL-JUNE 2012

[2] C. Deyan and Z. Hong, "Data Security and Privacy Protection Issues in Cloud Computing," in International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012 pp. 647-651.

[3] 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 Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[4] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.

[5] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang and Bu Sung Lee,"TrustCloud: A Framework for Accountability and Trust in Cloud Computing," 2nd IEEE Cloud Forum for Practitioners (IEEE ICFP 2011), Washington DC, USA,pp 1-8.

[6] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008

[7] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.

[8] 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, 2011.

[9] 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 Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[10] Parakh A, and Kak S (2009). Online data storage using implicit security, Information Sciences, vol 179(19), 3323–3331.

[11] Li H, Dai Y et al. (2009), Identity-Based Authentication for Cloud Computing, M. G. Jaatun, G. Zhao, and C. Rong (Eds.): Cloud Computing, Lecture Notes in Computer Science, vol 5931, 157–166.

[12] Wang Q, Wang C et al. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol 22(5), 847–859.

[13] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[14] Amazon Cloud, http://aws.amazon.com

IJERT