**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 2, February 2014, pg.675 – 680***

**SURVEY ARTICLE**

# A Survey on Privacy-Preserving Techniques for Secure Cloud Storage

**Salve Bhagyashri[1], Prof. Y.B.Gurav[2]**

P.G Scholar, Department of Computer Engineering, PVPIT, Bavdhan, Pune[1]

Assistant Professor, Department of Computer Engineering, PVPIT, Bavdhan, Pune[2]

salvebhagyashri1@gmail.com [1]

ybgurav@gmail.com [2]

**Abstract— Cloud computing is the technology which enables obtaining resources like so services, software, hardware over the internet. With cloud storage users can store their data remotely and enjoy on-demand services and application from the configurable resources. The cloud data storage has many benefits over local data storage. . Users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. The problem is that ensuring data security and integrity of data of user. so here ,we are having public auditability for cloud storage that users can resort to a third-party auditor (TPA) to check the integrity of data . Here, this paper gives the various issues related to privacy while storing the user's data to the cloud storage during the TPA auditing. Without appropriate security and privacy solutions designed for clouds this computing paradigm could become a big failure. We are a giving privacy-preserving public auditing using ring signature process for secure cloud storage system. In this paper we are going to analyze various techniques to solve these issues and to provide the privacy and security to the data in cloud.**

**Index Terms— Cloud computing, Data storage, privacy-preserving, Security, Integrity.**

## I. INTRODUCTION

CLOUD COMPUTING is widely developed technology used in IT industries which provide services like resources, network access, infrastructure, platform, rapid resource elasticity as per user require. In cloud computing the data of user is centralized to the cloud. The user can access the services anytime, anywhere with having internet connection. NIST definition of cloud computing as:

"*Cloud computing is a model for enabling convenient, 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"*.[1]

Cloud storage is a prototype of networked online storage in which the data is stored in virtualized pools of storage that are generally given by the TPA. Cloud storage enables data stored remotely to be temporarily cached on desktop computers, mobile phones or other internet devices. The IT industries, individuals which are storing their data to the cloud in flexible manner having some benefits like avoidance of capital expenditure on personal maintenances, Hardware, software, relief of online burden of data storage [2].

Many users from remote location use services continuously so there may arise some issues like privacy, security, data integrity, dynamic updates. Every time it is not possible for user to check the data is being consistent which is stored on cloud storage. So user always wants to maintain data integrity and privacy. Cloud service providers are the separate entities that store

 

data and provide services to the user. But user does not know that the cloud service providers can misuse their data, and correctness of data put on risk [4]. The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. This problem is addressed and solve by giving public auditing for secure cloud.

To ensure the data integrity and to reduce online burden it is of importance to enable public auditing service for cloud storage, so that user may resort to third-party auditor (TPA) to audit the data. The TPA who has capabilities and expertise that can periodically check the integrity of the data stored in cloud. The user does not have the capabilities that the TPA has. The TPA check the correctness of data stored in cloud on behalf of user and maintain the integrity of data. Enbaling public auditing service will play an important role for privacy data security & minimizing the data risk from hackers. The TPA is the external party which can also view the data stored on cloud so does not give the guarantee of data privacy.

## II. PRIVACY IN CLOUD STORAGE

Cloud provides many services like in online marketing, banking and payment, healthcares, social media as per use of personal information. Those privacy-sensitive data are residing in the other side of the globe. This movement highlights concerns on privacy and security in the cloud like how privacy of users is protected and perceived. For these growing privacy treats, many technologies have been proposed. The governments in the world are preparing lawful frameworks to protect security and privacy.

### *A. Something About Privacy*

Privacy is the preservation of the personal information of the cloud user. The cloud user can store their data and be worry free of the data security. Privacy means that the person to be free from all disruption.
The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define about the privacy as:

*"Privacy is the right and obligation of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information".*

### *B. Issues in cloud storage about Privacy and security*

Considering the privacy risk of user data in cloud storage, it is important as privacy threats vary according to what type of cloud scenario. The following issues are addressed in cloud storage:

- The treats against information assets residing in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- The security risks associated with the cloud, and where relevant considerations of attacks and Countermeasures.
- Emerging cloud security risks.
- Some example cloud security incidents.

Some other issues like lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, lack of user control, addressing transborder data flow restrictions, legal uncertainty, compelled disclosure to the government, data accessibility, location of data, transfer and retention, data security and disclosure of breaches.[3][5]

## III. SOLUTIONS FOR THE PRIVACY PROBLEMS BASED ON VARIOUS TECHNIQUES

A cloud computing is a distributed computing system which provides delivery of computing services over the internet. There are three service models in cloud computing which include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).Cloud computing is presently one of the popular concept in IT companies. The cloud storage stores large amount of data which does not offer guarantee on data integrity and consistency. So the user don't having belief about the privacy of user data because the cloud storage can also misuse the data of user. For privacy and security concerns the user resorts to TPA to maintain the data security. But the TPA can't give the guarantee of data privacy of user. For the privacy and security of data, the user has to encrypt their important data before storing into the cloud storage. But in traditional encryption their exist some drawback. When the owner of the secret key want to see the data stored on cloud storage at that time he may need to download all encrypted data from cloud storage and then decrypt it and after that find the data which he needs. When the encrypted data is very large at his condition it will be inconvenient. This causes the serious trouble to the user.

 

In "Provable Data Possession" (PDP) model ensures the possession of data files on untrusted storages [6]. This technique is used to permit a client to frequently, efficiently and securely verify the server who stores client potentially very large amount of data. That is the server might delete some part of the data or it might not store all data in cloud storage. PDP is a public key based technique which allows any verifier to query the server and POR verifies the integrity of cloud data using special blocks called sentinels. But this model discloses the information of user to the external parties and the privacy gets violated.

Juels et al.[7]gives" proof of retrievability"(POR)model in which error correcting codes are used for retrievability of data file on service .But every time the user does not possible to check the data, which introduce burden to the user. This POR is used for only encrypted data, but we are introducing privacy-preserving public auditing for secure cloud storage independent to encryption, so this concept does not works. Shacham and Waters[8] gives an improved POR scheme with improved security concept built from BLS signatures. But this concept is not good for privacy-preserving.

Shan et al.[9]introduce TPA concept to reduce online burden and keeps the privacy-preserve.

Chen et al.[10] gives mechanism for auditing the correctness of data with multiple server.

For secure cloud different framework, techniques, methodologies, protocols have been proposed. In this paper, we classify the techniques into three groups as like Encryption method, Access Control Mechanism and Auditability Schemes which gives assurance of privacy and security and which methodology is good one.

### *A. Encryption Methods:*

Different approaches for encryption are given here to maintain the privacy of the user data. The design of privacy-preserving cloud storage framework to solve privacy problem is given by RuWei et.al [11], this comprises the design of the generation and management of keys, data organization structure, the interaction between participants and the handling of change of use's access right. It uses an interactive protocol. The algorithm used in this is an extirpation based key derivation algorithm. It ensures data consistency, solve ineffectiveness of key derivation, reduces the burden of encryption and decryption of data owner, can be able to manage numerous keys, confidentiality, storage space gets reduced, required time gets reduced. This concept of RuWei provides good security and privacy to the user data and it is appeal to multiple users. Though this concept is good one but it increases the owner's encryption liability. So, for that we need to work on cipher text.

A technique for to make better user privacy with secret key recovery in cloud data storage that permits users to encrypt their files in the cloud storage[12]. A Secret sharing Algorithm to Key Recovery Mechanism is used. A privacy-preserving cloud storage framework supporting cipher text retrieval is given by RuWei et.al in [13], it is used to solve the problems while operating on an encrypted data. This also minimizes user's workload on management of data. The algorithm used here is Key derivation Algorithm, Interaction protocol, combination of symmetric and asymmetric encryption and Bloom Filter.

The Fan, C.I., and Huang[14] gives concept of privacy search process. This concept includes revocable delegated search and un-decryptable delegated search that are based on symmetric predicate encryption in the cloud data storage.

There is some drawback of this encryption method as like it increases the burden and limits on the usage of data. Such type of drawback gets eliminated by introducing Access Control Mechanism explain below.

### *B. Access Control Mechanism*

A privacy preserving authenticated access control scheme is used for security of user data in cloud storage.

This concept is used to identify the authenticity of the user without knowing the user's identity before storing information [15]. Only valid users are able to decrypt the stored data. It preserves the privacy of data; maintain the security and keeps secrete the identity of user.

### *C. Auditability schemes*

Auditing process not only motivates to providers to improve their services but also reduces the online burden. The auditing is of two types like **Public Auditability** and **private Auditability.** The private auditability gives higher efficiency. The public auditability enables everybody like users, customers to interact with cloud server or cloud storage. So here for consistency and privacy user may resort to TPA. The auditing protocols are like **Third Party Auditing** and **Data Owner Auditing.** The framework for cloud data storage is given below:

 

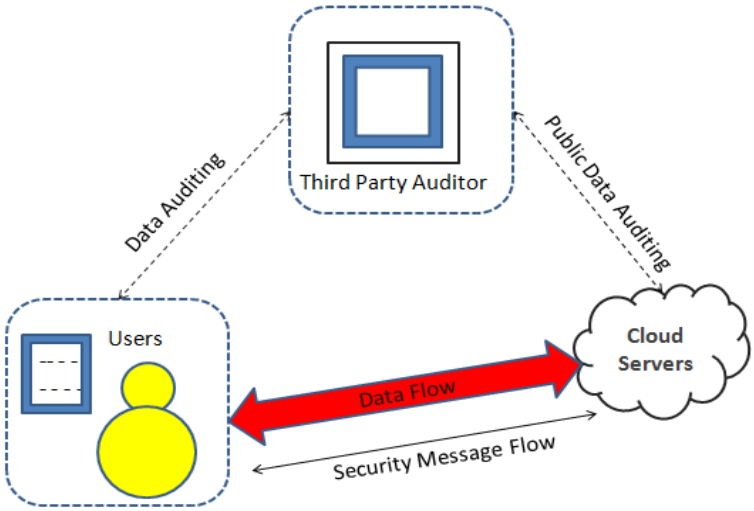


Fig.1. The framework of cloud data storage.

As shown in figure, the model consist three different entities: the *cloud user, the cloud server* (CS) *and the third- party auditor* (TPA).The *cloud user* is the one who has large amount of data files that are stored in the cloud; the *cloud server* is the one who provides the data storage service like resources, software to the user. The cloud server is managed by cloud service provider; the *third- party auditor* is the one who has trusted to access the cloud storage service on behalf of user whenever user request for data access. The TPA has capabilities and expertise that the user does not have. They can also interact with cloud server to access the stored data for different purpose.
The two basic schemes for auditing are MAC (Message Authentication Code) based solution and HLA (Homomorphic Linear Authenticator) based solution given below:

MAC-Based solution: It is used to authenticate the data which is stored on cloud server. The data file *F* is divided into number of data blocks and the data blocks having their MAC with keys. In this scheme we uploading the data blocks with their MACs to the server and it send the secret key *sk* to the TPA .After that the TPA retrieve data blocks which is having MACs by using secret key *sk*, and verify the correctness of the data. This MAC based solution has some drawbacks: 1)It increases the online burden to users because every time it is not possible for TPA to verify the secret key *sk*.2)The data file which is audited number of times is limited by the number of secret keys.3)It supports only static data not for dynamic.

HLA-Based Solution**:** The HLA technique can be used for public auditing without retrieving the data blocks themselves. In this solution user authenticates each element of file *F* after that the TPA verifies cloud storage by sending random set of challenge. This technique is also not suitable for our auditing process because the linear combination of blocks may show user information to TPA which comply with privacy-preserving. So this drawback is not useful for our privacy-preserving auditing process.
Comparison of Other schemes for public auditing is given here:

- *Remote Data Possession at Untrusted Host*

Chen, L., and Guo[16], have been proposed with the goal of remote data possession checking schemes. This concept explains an efficient RDPC scheme which is efficient in terms of computation and communication. It permits the challenger to do verification without comparing against the original data; it includes small challenges and responses, and users need to store only two secret keys and several random numbers.

- *Public Verifiability For Storage Security*

The data integrity and consistency is the main issue in cloud storage. The cloud server has to ensure the data integrity and data consistency. To maintain the data integrity the user may resort to TPA. So the TPA performs the auditing on behalf of the user and reduces online burden [17].

- *Data Integrity Checking For Privacy-Preserving*

A privacy preserving remote data integrity checking protocol with public verifiability and data dynamics make use of a Remote Data Integrity Checking Protocol. This protocol provides public verifiability without the help of a third party auditor. It doesn't disclose any user information to third party auditor.

 

- *Privacy-Preserving Public Auditing For Secure Cloud Storage*

In this Scheme homomorphic linear authenticator (HLA) is integrated with random masking technique. The data file which is having linear combination of sampled blocks is masked with randomness generated by the server. This linear combination of blocks is given by the server's response. In random masking technique the block has chosen randomly. In this scheme, HLA is indicated with random masking, the TPA can't see the information to build up correct group of linear equation. Due to this scheme the TPA does not see the user's information or data. This Scheme uses public key -based HLA.The privacy-preserving public auditing process runs into two phases, setup and audit. Some advantages of this scheme are as:

1. Privacy-preserving: TPA can't see the users data content during the auditing process.
2. Public Auditability: To allow TPA to verify the correctness of cloud data without retrieving the copy of whole data.
3. Batch Auditing: TPA handles multiple users during auditing process.
4. TPA performs auditing process with minimum communication.

- *Privacy-preserving Public Auditing Using Ring Signature scheme*

To maintain more data integrity and privacy Ring Signatures concept we are giving here. The concept of ring signatures is first proposed by Rivest et al. in 2001[7]. The ring signature is the type of digital signature which can be performed by any group member of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. The best properties of a ring signature are that it should be difficult to determine *which* of the group members' keys was used to produce the signature. In this, the signature is computed using one of the group member's private key, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier. The name "ring signature" comes from the ring-like structure of the signature algorithm. In privacy-preserving public auditing scheme, the TPA verify the integrity of data without retrieving the whole data, but in ring signature concept during auditing process, the identity of signer on each block of data is kept private .

## IV. CONCLUSION

Cloud computing is a technology which is used worldwide through the internet. The main point in this paper is privacy and security issue. This problem we tackle in this paper. We give here many privacy and security issues and solution on this issue. Different techniques and methods we are given here to solve the problems of privacy of user data. This paper has addressed some privacy approaches for overcoming the issues in privacy on untrusted data stores in cloud computing. We categories the methodologies as encryption based methods, access control based mechanisms and auditability schemes. Thus, we need to develop privacy–preserving framework that overcomes the worries in privacy security and encourage users to adopt cloud storage services confidently.

## REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of cloud computing," http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, June 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Comput- ing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[3] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.

[4] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010

[5] Mohammed, A., AlSudiari, T., & Vasista, T. G. K. 2012. Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications.Advanced Computing: An International Journal (ACIJ), 3 (2), 159-169.

[6] Ateniese, G., Burns, R., Curtmola, R., Herring, J.,Kissner, L., Peterson, Z., & Song, D. 2007, October. Provabledata possession at untrusted stores. InProceedings of the 14th ACM conference on Computer and communications security (pp. 598-609). ACM.

[7] 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.

[8] H. Shacham and B. Waters, "Compact Proofs of r etrievability,"Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008

[9] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

 

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Sys-tems," in *Proc. ACM*

[11] Huang, R., Yu, S., Zhuang, W., & Gui, X. 2010. Design of privacy-preserving cloud storage framework. In Grid and Cooperative Computing (GCC), 2010 9th International Conference on (pp. 128-132). IEEE

[12] Huang, Z., Li, Q., Zheng, D., Chen, K., & Li, X. 2011, December. YI Cloud: Improving user privacy with secret key recovery in cloud storage. In Service Oriented System engineering (SOSE), 2011 IEEE 6th International Symposium on (pp. 268-272). IEEE.

[13] Huang, R., Gui, X., Yu, S., & Zhuang, W. 2011. Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. In Network Computing and Information Security (NCIS), 2011 International Conference on(Vol. 1, pp. 93-97). IEEE.

[14] Fan, C. I., & Huang, S. Y. 2012. Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Generation Computer Systems.

[15] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid),12th IEEE/ACM International Symposium on(pp. 556-563). IEEE.

[16] Chen, L., & Guo, G. 2011. An efficient remote data possession checking in cloud storage. International Journal of Digital Content Technology and its Applications,5(4), 43-50.

[17] Gohel, M., & Gohil, B. 2012. A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage. Trust Management VI, 240-246.

[18] Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W. 2010. Privacy-preserving public auditing for secure cloud storage.

 