Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Review on Privateness-Retaining Public Auditing for Secure Cloud Storage

Mukta Bhatele
Head of Department
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Deepika Gour
Research Scholar
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:deepika.gour.1990@gmail.com

B. L. Rai
Associate Professor
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:blrai_08_76@yahoo.co.in

Ankur Pandey
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P), [India]
Email :- ankur.pandey1205@gmail.com

Abstract*—In cloud computing, one of the core design principles is dynamic scalability, which guarantees cloud storage service to handle growing amounts of application data in a flexible manner or to be readily enlarged. By integrating multiple private and public cloud services, hybrid clouds can effectively provide dynamic scalability of service and data migration. Security plays a vital during the transmission of data from the sender to the receiver in any environment. Data integrity is the storing of data from many nodes to a particular place. The concept of cloud has been introduced for the data integrity and data storage. But when a number of clouds have been implemented and the data is stored dynamically then the verifiability of the node from one cloud to another is typical to achieve and the security of the data dynamics is also difficult to achieve. In this paper we are presenting a survey of privacy preservation in cloud storage. We also discuss various method proposed by various researchers.*

Keywords:— *Privacy preservation, Public varifiability, cloud storage, hybrid cloud.*

1. INTRODUCTION

The Internet is becoming an increasingly vital tool in our everyday life for professional and personal users and them becoming more numerous. In the current trends business is progressively more conducted over the Internet. And in the area of internet cloud computing is one of the most revolutionary concepts of recent years. Cloud computing is the latest emerging computing technology where platform, data storage and IT services are provided over the internet. Due to vast availability of resources and numerous tasks being submitted to the task management becomes important for optimal scheduling which affects the efficiency of the whole cloud computing environment. The use of Cloud Computing is gaining popularity due to its mobility and massive availability in minimum cost. On the other side it comes with more threats to the security of the company's data and information. In current scenario data mining techniques are most using technique. The Cloud Computing provides its users benefit of unprecedented access to valuable data that can be turned into valuable insight

that can help them achieve their business objectives.

Cloud computing has been visualized as the next generation information technology (IT) construction for enterprises, due to its long list of extraordinary advantages in the IT history like; ubiquitous network access, on-demand self-service, location sovereign resource pooling, usage-based pricing, rapid resource elasticity and transference of risk [1] [2]. Data mining in cloud computing is the process of extracting structured information from unstructured or semi-structured web data sources. It permits organizations to consolidate the management of software and data storage, long with guarantee of reliable, efficient and secure services for their users.

Internet-based online services provides huge amounts of storage space and customizable computing resources, such computing stage shift, although is removing the liability of local machines for data maintenance at the similar time. Due to this users are at the mercy of their cloud service providers for the availability and integrity of their data. So the security of data is an significant aspect of service quality. In case of cloud computing scenario the traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users loss control of data. As a result, authentication and verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

As cloud computing permits individuals to store the data remotely, it has competence of enabling end users to use the resources provided in an inflexible way. The benefits of cloud computing is it provides on demand self service methodology that authorizes users to request resources dynamically. Data owners store data on a cloud computing storage provider remotely and they cannot directly use conventional cryptographic algorithm to guarantee security for data. And downloading data for integrity verification costs high and even huge data transmission through network regularly may support customers economically. Once if the data has been stored on cloud computing data storage provider data owner should not concern about security of data. In order to guarantee security for data and to enable data owner to use data without any worry about security for data; publicly auditable cloud storage providers where data owners can rely on third party auditor to verify the data integrity of out sourced data to ensure security [3].

Representative network architecture for cloud data storage is shown in Figure 1. There are various network entities can be identified as client, cloud storage server and third party auditor. Client is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and calculation, can be moreover individual consumers or organizations. Cloud Storage Server (CSS) is an entity that is supervised by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data. Third Party Auditor (TPA) is an entity, which has expertise and capabilities that clients do not have, is faithful to assess and investigate risk of cloud storage services on behalf of the clients upon request [3].

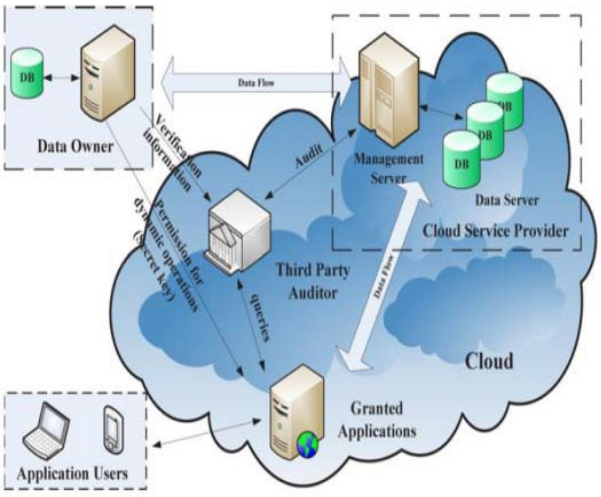

Figure 1: Audit system architecture for cloud computing

The general definition of an audit is a planned and documented activity performed by qualified personnel to determine by

examination or investigation or valuation of objective confirmation, the satisfactoriness and compliance with recognized procedures or appropriate documents, and the usefulness of implementation. To securely introduce an efficient TPA the auditing process should convey in no new vulnerabilities toward user data privacy and commence no extra online burden to user. Considering the large size of the outsourced data and the user's constrained resource competence, the tasks of auditing the data exactness in a cloud environment can be formidable and expensive for the cloud users [4]. Moreover, the overhead of using cloud storage should be minimized as much as possible, so as to a user does not require to achieve too many operations to use the data. In particular, users may not want to go through the complexity in verifying the data integrity. Moreover there may be many user accesses the same cloud storage, say in an enterprise setting. For simple management it is pleasing that cloud only considers verification request from a single designated party. To completely make certain the data integrity and protect the cloud users' computation resources as well as online load, it is of critical significance to facilitate public auditing service for cloud data storage so that the users may alternative to an autonomous third-party auditor (TPA) to audit the outsourced data when needed [1].

To ensure cloud data storage security is critical to permit a TPA to calculate the service quality from an objective and independent perspective. Public audit ability also allows clients to delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications [4]. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud. The TPA, who has expertise and capabilities that users do not have, can timely make sure the integrity of all the data stored in the cloud on behalf of the users that offers a much more easier and reasonably priced way for the users to ensure their storage correctness in the cloud. Furthermore, in addition to help users to estimate the risk of their subscribed cloud data services and the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service standard and even provide for autonomous arbitration purposes [5].

Privacy-Preserving is used to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process. The privacy-preserving public auditing is uniquely integrate the homomorphic non-linear authenticator with random masking technique. In the non-linear blocks in the server's response is masked with randomness produced the server. With random masking, the TPA no further has all the necessary information to build up a correct group of non-linear equations and therefore cannot derive the user's data content, no substance how countless linear combinations of the same set of file blocks can be together. Besides the correctness justification of the block authenticator pairs can still be carried out in a new way even with the presence of the randomness [6]. With the establishment of privacy- preserving public auditing, the TPA may at the same time as handle numerous auditing upon different users entrustment. The individual auditing of these assignments for the TPA can be tedious and very inefficient.

From the perspective of protecting data privacy, the users, who have possession of the data and rely on TPA just for the storage security of their data and users do not desire this auditing process initiating new vulnerabilities of unauthorized information leakage towards their data security. To effectively support public audit ability without having to retrieve the data blocks themselves the homomorphic authenticator technique were used. Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks that can be strongly aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the

aggregated authenticator. Furthermore, the direct adoption of these methods is not suitable since the linear combination of blocks may potentially reveal user data information, consequently violating the privacy-preserving assurance. Particularly, if sufficient number of the linear combinations of the same blocks is composed, the TPA can simply obtain the user's data content by solving a system of linear equations [7].

Overview to achieve privacy-preserving public auditing uniquely integrate the homomorphic authenticator with random mask technique was used. With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concomitantly deal with multiple auditing delegations upon different users requests. The being auditing of these goals for TPA can be tedious and very inefficient. The rest of paper is organized as follows. In Section II describes about background of privacy preservation public auditing. Section III describes about related work. Section IV describes about conclusion.

2. BACKGROUND

Cloud Computing is continuously evolving and showing consistent growth in the field of computing. Excluding, the security issues and threats linked with it still stay as a cumbersome. Cloud data storage can be affected by two different sources. The cloud data storage provider itself is untrusted and possibly malicious. There are cases in corrupting the data that is stored by users on individual servers. An adversary can compromise an individual server pollute the original data files by modifying or even by introducing its own fraudulent data to prevent the original data from being retrieved by the user. Preserving the privacy of user, his identity and data in the cloud is very mandatory.

The data owners could no longer physically possess the storage for their data; developer cannot directly adopt cryptographic primitives to ensure the data security because downloading data every time for the purpose of integrity verification is not a feasible solution to be followed by the data owners as it is economically cannot be afforded by them. On the other side, detecting data corruption only when accessing data does not give assurance of the correctness of data, if the data size is too large. To overcome all of these challenges there is a need of third party auditing to ensure data security completely and save data of owners. It is important, that the privacy has to be preserved anytime and anywhere.

3. RELATED WORK

This section describes some related work to privacy preservation public audit for secure data storage.

Cong Wang et al [1] propose a privacy-preserving public auditing system for data storage security in cloud computing. They utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process that not only removes the burden of cloud user from the tedious and possibly expensive auditing task, although also assuages the users' fear of their outsourced data escape. Taking into consideration TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, they further extend our privacy-preserving public auditing protocol into a multiuser situation, where the TPA can execute numerous auditing tasks in a batch manner for better efficiency [1].

To accomplish privacy-preserving public auditing, they suggest to uniquely integrating the homomorphic linear authenticator with random masking method. In this protocol, the linear combination of sampled blocks in the server's reaction is masked with randomness generated by the server. With random masking, the TPA no longer has all the essential information to construct up a accurate group of linear equations and for that reason cannot derive the user's data content, no issue how many linear combinations of the identical set

of file blocks can be composed. Alternatively, the rightness corroboration of the block-authenticator pairs can still be accepted in a new way even with the occurrence of the randomness. Their design makes employ of a public key-based HLA, to provide the auditing protocol with public auditability [1].

By integrating the HLA with random masking, this protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server (CS) during the efficient auditing procedure. The algebraic and aggregation properties of the authenticator further benefit of this design for the batch auditing. This public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. This scheme enables an external auditor to audit user's cloud data without learning the data content. This also supports scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner [1].

They consider a cloud data storage service involving three various entities, as shown in figure 2: the user who has big amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources the third-party auditor that has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon demand. Users are dependent on the CS for cloud data storage and preservation. They may also vigorously work together with the CS to access and update their stored data for various application intentions. As users no longer possess their data in the neighborhood, it is of critical importance for users to ensure that their data are being correctly stored and maintained. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, whereas hoping to keep their data confidential from TPA [1].

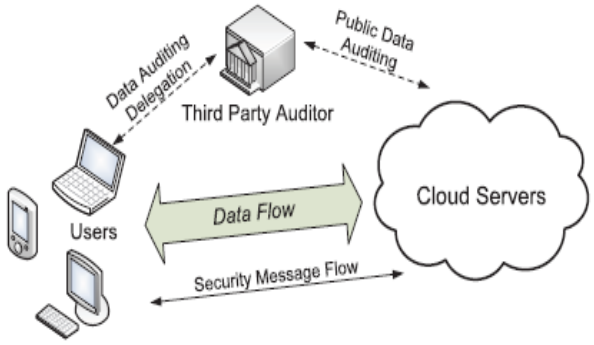

Figure 2: The architecture of cloud data storage service.

Swathi Sambaing proposed publicly auditable cloud storage providers where data owners can rely on third party auditor to verify the data integrity of sourced data to make sure security. To considerably diminish the arbitrarily large communication overhead for public auditability without commencing any online burden on the data owner, they resort to the homomorphic authenticator technique. Homomorphic authenticators are extraordinary metadata generated from individual data blocks that can be securely aggregated in such a way to guarantee a verifier that a linear combination of data blocks is properly computed by verifying only the aggregated authenticator. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. To address this concern, a proper approach is to combine the homomorphic authenticator with random masking. This way, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the owner's data substance, no issue how many linear combinations of the same set of file blocks can be collected [3].

Meanwhile, due to the algebraic property of the homomorphic authenticator, the exactness validation of the block-authenticator pairs (μ and σ) can still be carried out in a new way, even in the presence of randomness. This improved technique ensures the privacy of owner data content during the auditing process, regardless of whether or not the data is encrypted, which definitely provides more flexibility for different application scenarios of cloud data storage. Besides, with the homomorphic authenticator, the desirable property of constant communication overhead for the server's response during the audit is still preserved [3].

Q. Wang et al [4] explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing. In view of the key role of public auditability and data dynamics for cloud data storage they propose an efficient construction for the seamless integration of these two components in the protocol design. They offered a protocol supporting for fully dynamic data operations, especially to support block insertion, which is missing in most existing schemes. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies. In case those clients do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA. They only consider verification schemes with public auditability: any TPA in possession of the public key can act as a verifier [4].

They [4] assume that TPA is unbiased while the server is un-trusted. For application purposes, the clients may interact with the cloud servers via CSP to access or retrieve their pre stored data. More importantly, in practical scenarios, the client may frequently perform block-level operations on the data files. The most general forms of these operations are modification, insertion, and deletion. To effectively support public auditability without having to retrieve the data blocks themselves, they resort to the homomorphic authenticator technique. The naive way of realizing data integrity verification is to make the hashes of the original data blocks as the leaves in MHT, so the data integrity verification can be conducted without tag authentication and signature aggregation steps. So they adopt the block less approach, and authenticate the block tags instead of original data blocks in the verification process. To achieve efficient data dynamics, they improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the scheme is highly efficient and provably secure [4].

M.A. Shah et al [5] proposed solution to offer storage service accountability is throughout independent, third party auditing and arbitration. The customer and service enter into an agreement or contract for storing data in which the service provides some type of payment for data loss or failing to return the data intact, e.g. free prints, refunds, or insurance. In such a contract, the two parties have contradictory incentives. The service provider, whose objective is to make a profit and preserve a reputation, has an incentive to hide data loss. On the other hand, customers are terribly untrustworthy, e.g. casual home users. Customers can innocently or fraudulently claim loss to get paid. Thus, they engage an independent, third party to arbitrate and confirm whether stored and retrieved data is intact. This protocol has three important operations, initialization, audit, and extraction.

For audits, the auditor interacts with the service to check that the stored data is intact. For extraction, the auditor interacts with the service and customer to check that the data is intact and return it to the customer [5].

This protocol shift the burden of maintenance these secret keys to a storage service. Since services are already in the business of maintaining customers' data and privacy, the keys are safer with them. Keeping the data content confidential from the service is discretionary. A customer can keep the keys and encrypted data with the same service, thereby enlightening the contents to that service and allowing it to offer value-added features away from storage like search. Otherwise, the customer can separate the keys and encrypted data onto non-colluding services to maintain complete privacy. The auditor is responsible for auditing and extracting both the encrypted data and the secret keys. Although they present the protocols for handling the encrypted data for wholeness, they are straightforward extensions of existing techniques. They also describe methods for privacy preserving auditing and extraction of digital contents. These schemes separate the data into two pieces, an encryption key and the encrypted data. This protocols consent to an auditor, with minimal long-term state, to audit both those pieces and extracts those pieces without revealing the fundamental contents of either. Using this protocol, all these properties can be achieved without requiring the customer to maintain any long-term state. The protocols for the encrypted data rely on cryptographic hashes and symmetric key encryption [5].

Srinivas, D. propose a privacy-preserving public auditing system for data storage security in Cloud Computing. He tries to utilize the homomorphic non-linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process that not only reduces the burden of cloud user from the tedious and possibly pricey auditing task, but also alleviates the users' terror of their outsourced data security. Taking into account TPA may concurrently handle multiple audit sessions from dissimilar users for their outsourced data files, he further extend this privacy-preserving public auditing protocol into a multi-user scenario, where the TPA can perform multiple auditing tasks in a batch manner for better effectiveness. Extensive examination shows that this schemes are almost certainly secure and highly efficient [6].

In year 2010, Wang, Cong et al [7] offered Privacy-preserving public auditing for data storage security in cloud computing. This work is among the first few ones to sustain privacy-preserving public auditing in Cloud Computing, with a spotlight on data storage. Above and beyond, with the occurrence of Cloud Computing, a predictable increase of auditing tasks from diverse users may be delegated to TPA. As the entity auditing of these growing tasks can be tedious and unwieldy, a natural demand is then how to enable TPA to efficiently perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Allowing for TPA may concurrently handle multiple audit sessions from different users for their outsourced data files [7].

In 2008 by Stephen S. Yau, et. al [8] gives a concept about warehouse for integrating data from various data sharing services without central authorities is existing with our warehouse, data sharing services can update and control the access and limit the usage of their shared data, as a substitute of submitting data to establishment, and our repository will support data sharing and addition. The main differences between their storehouse and existing central authorities are: 1) repository collects data from data sharing services based on users' integration requirements rather than all the data from the data sharing services as existing central establishment. 2) While existing central establishment have full control of the collected data, the capability of warehouse is controlled to computing the integration results required

by users and cannot get other information about the data or use it for other work. 3) The data composed by warehouse cannot be used to generate other results except that of the specified data addition request, and, hence, the cooperation of warehouse can only reveal the results of the specified data integration demand, while the compromise of central establishment will reveal all data and presented a privacy preserving repository to integrate data from various data distribution services. In contrast to existing data allocation techniques, warehouse only collects the least amount of information [8].

In 2009 Qian Wang et al [9] introduced a new scheme which gives remote data integrity and verifiability means dynamic data operations. The method initially identifies the troubles and potential security problems of direct extensions with fully dynamic data updates. It achieves efficient data dynamics and improves the Retrieve ability model by manipulating the classic Merkle Hash Tree (MHT) construction used for block tag validation. It is extremely proficient and secure technique [9]. In 2010 Yan Zhu, Huaixi et al [10] proposed data possession scheme in hybrid clouds which supports scalability of service and data immigration. It permits the scenario of numerous cloud service providers to cooperatively store and maintain the clients' data. This scheme gives less overhead and reduces communication complexity.

In 2009 Qian Wang et al [11] introduced a protocol Which firstly identify the difficulties and potential security problems of direct extensions with fully dynamic data updates and secondly shows how to construct an elegant verification scheme for faultless integration. It influences the classic Merkle Hash Tree (MHT) construction for block tag validation [11]. Ateniese et al. [12] are the first to consider public auditability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor [12].

Juels et al. [13] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data [13]. Miao Zhou et al. [14] considered the privacy of users in the cloud environment and proposed a flexible method of access control. Each cloud user is linked with certain attributes, which determines their access rights. The paper propounded a two-tier encryption model in which the base phase and surface phase builds up the two tiers of the model respectively. At the first phase, the data owner performs local attribute-based encryption on the data that has to be outsourced. The surface phase on the other hand is performed by the cloud servers, after the initialization done by the cloud data owner. This phase implements the Server re-encryption mechanism (SRM). The SRM dynamically re-encrypts the encrypted data in the cloud, when the owner of that data requests. The request for SRM arises either when a new user has to be created or an existing user has to be repealed. Though the re-encryption takes place in cloud server, the privacy of users data is not compromised as the access policies remains hidden to the cloud servers [14].

5. CONCLUSION AND FUTURE WORK

The cloud computing has rapidly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Security and privacy,

however, are a concern for agencies and organizations considering migrating applications to public cloud computing environments. The Cloud security responsibilities can be taken on by the customer, if he is managing the cloud, but in the case of a public cloud, such responsibilities are more on the cloud provider and the customer can just try to assess if the cloud provider is able to provide security. Public auditability also allows clients to delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications. In this paper, some of the privacy preservation and public audits are addressed and the techniques to overcome them are surveyed. While some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy.

ACKNOWLEDGMENT

I would like to thank Dr. Mukta Bhatele, for accepting me to work under his valuable guidance. He closely supervises the work over the past few months and advised many innovative ideas, helpful suggestion, valuable advice and support.

REFERENCES:

[1] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, pp. 362 – 375, February 2013.

[2] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[3] Swathi Sambangi "Cloud Data Storage Services Considering Public Audit for Security", Global Journal of Computer Science and Technology Cloud and Distributed, ISSN: 0975-4172, Vol. 13, Issue 1, pp. 1 – 6, 2013.

[4] 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, May 2011.

[5] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[6] Srinivas, D. "Privacy-Preserving Public Auditing In Cloud Storage Security." International Journal of computer science and Information Technologies,ISSN: 0975-9646, vol. 2, no. 6, pp. 2691-2693, 2011.

[7] Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in cloud computing." In proceedings of 2010 IEEE INFOCOM, pp. 1-9, 2010.

[8] Stephen S. Yau, Fellow And Yin Yin "A Privacy Preserving Repository For Data Integration Across Data Sharing Services", IEEE Transactions On Services Computing, Vol. 1, No. 3, July-September 2008.

[9] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", 2009 Proceedings of the 14th European conference on Research in computer security (ESORICS'09), pp. 355-370, 2009.

[10] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen

S. Yau, "Efficient Provable Data Possession for Hybrid Clouds" Proceedings of the 17th ACM conference on Computer and communications security (CCS'10), pp. 756-758, october 2010.

[11] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" Proceedings of the 14th European conference on Research in computer security (ESORICS'09), pp. 355-370, 2009.

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

[13] 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.

[14] Zhou, Miao, Yi Mu, Willy Susilo, Man Ho Au, and Jun Yan. "Privacy-preserved access control for cloud computing." In proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 83-90, 2011.