(IJRST) 2016, Vol. No. 6, Issue No. I, Jan-Mar e-**ISSN: 2249-0604; p-ISSN: 2454-180X**

PRIVACY-PRESERVING PUBLIC AUDITING FOR REGENERATING-CODE-BASED CLOUD STORAGE

***Ms. C.Jeevitha, ** Dr. T. Senthil Prakash, * Ms.C.Janani**

**II year ME (CSE), Shree Venkateshwara Hi-Tech Engg College, Gobi*
***Professor & HOD, Shree Venkateshwara Hi-Tech Engg College, Gobi*

ABSTRACT

Data integrity maintenance is the major objective in cloud storage. It includes audition using TPA for unauthorized access. This work implements protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Proxy server. The data of the users will be stored in public and private area of the cloud. So that only public cloud data will be accessed by user and private cloud will remain more secured. Once any unauthorized modification is made, the original data in the private cloud will be retrieved by the Proxy server and will be returned to the user. Every data stored in the cloud will be generated with a Hash value using Merkle Hash Tree technique. So modification in content will make changes in the Hash value of the document as well. Proxy also perform signature delegation work by generating private and public key for every user using OEAP Algorithm so that the security will be maintained. In our proposed we implement this scenario in a multi owner environment in which one document will be access by user groups. In this context, the access limit should be properly maintained so that no user for other group should be allowed to modify a particular group's data. Also, if any modifications made in that data, it will be informed to the user as well by the proxy.

1. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to it is intrinsic resource sharing with low maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon and others are able to deliver various service to cloud users with the help of powerful data centers. By shifting the local data management systems into cloud servers and users may enjoy high quality services and save significant investments on them local infrastructures. One of the most fundamental services are offered by cloud providers was data storage. Let's consider a limited data application the company allows its staffs in the same group or department to stored and shared files in the cloud. By utilizing the cloud that the staffs could be completely released from the troublesome local data storehouse and maintenance. However, it is also poses a significant risk to the confidentiality of those stored files. Specifically the cloud servers is managed by cloud providers is not fully trusted by users while the data files stored in the cloud might be confidential and sensitive such as business plans. To preserves data privacy is primary solution for encrypt data files and then uploaded the encrypted data into the cloud [2]. Unfortunately, the

designing of the efficient and secure data sharing scheme for groups in the clouds is not an easy task due to the following challenging issues.

First of all identity the privacy is being one of the most significant restriction for the wide deployment of cloud computing. Here not holding the guaranteed of identity privacy user may be unwilling to append in cloud computing systems because their real identities can be easily disclose to cloud providers and also attackers. On the other hand its unconditional identity privacy might incur the abuse of privacy for example the misconduct staff could deceive others on the company to sharing false files without being traceable. Therefore, traceability and which are enables the TPA to expose the real identity of a user's are also highly desirable.

Second, it is highly recommended that any member in the groups should able to fully enjoy the data storing as well as sharing services provided by the cloud which are defined as the multiple owner manner. Compare with the single owner manner where only the group manager could store and modify data in the cloud, the multiple owner manners are more flexible in practical applications. More concretely, each users in the groups are able to not only read data and also modify his or her part of data in the entire data file shared to the company. Last but not the least so that groups are normally dynamic in practice, e.g., new staff cooperation and current employee revocation in the company. The changes of membership makes secure data sharing extremely problematic. On one hand, the anonymous systems can challenges modern granted users can learn the content of data files stored before their cooperation, because it is not possible for new granted users to contact with anonymous data owners and access the corresponding decryption keys. On the other hand the efficient membership repeal mechanism without updating the classified keys of the remaining users has also desire to minimize the complexity of key management. Many security schemes for data sharing on untrusted servers had been proposed. In these approaches, data owners are able to store the encrypted data files in mistrustful storage with distributed the corresponding decryption keys are only to authorized users. Thus, unauthorized users as well as storage servers could't learn the content of the data files because they don't have knowledge of the decryption keys.

However, the complexity of user participation and repeal in these schemes are linearly increasing with the numbers of data owners as well as the number of revoked users, respectively. By setting the group with a single attribute, we proposed a secure provenance scheme is established on the cipher text policy attribute established encryption technique, which are allows any member in a group to share data with others. However, the issue of user revocations is not addressed in their scheme. We presented a scalable and fine grained data access control scheme on cloud computing based on the key policy attributes based on by encryption technique with the implementation of Proxy Server. Unfortunately, the single owner manner hinders the adoption of theirs scheme into the case, where all users are granted to store and share data. Hence we are implementing a group based

Data owner system.

2.OVERVIEW

The main aim of the project is to support dynamic groups efficiently. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature or group master key and dynamic broadcast encryption techniques.

Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. The proxy server computes the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overhead of users for encryption operations and the cipher text size is constant and independent of the revocation users. The proxy maintain the signature delegation work which generates the private and public key of each group so that the permission for the access of file can be restricted. Revocation is user is performed if any user make unauthenticated action on any data in the cloud. Also if a data has been modified by the user it will be detected, penalized and the code will be regenerated by the proxy.

In this the user revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The list is characterized by time stamp t1,t2,…tr. In the proposed system once the user time stamp over does not wait for the group manager to update the time stamp or revocation list here once the time over the user immediately send request for extra time for access the data to the cloud. Then the cloud will send that request to the group manager once the see it and give permission then the cloud will time to access the data but if the group manager did not give permission then the cloud will not give permission for access of the data.

3.RELATED WORKS

Advances in networking technology and an increase in the need for computing resources have prompted many organizations to outsource their storage and computing needs. This new economic and computing model is commonly referred to as cloud computing and includes various types of services such as: infrastructure as a service (IaaS), where a customer makes use of a service provider’s computing, storage or networking infrastructure; platform as a service (PaaS), where a customer leverages the provider’s resources to run custom applications; and finally software as a service (SaaS), where customers use software that is run on the provider’s infrastructure. Cloud

infrastructures can be roughly categorized as either private or public. In a private cloud, the infrastructure is managed and owned by the customer and located on-premise (i.e., in the customer's region of control). In particular, this means that access to customer data is under its control and is only granted to parties it trusts. In a public cloud the infrastructure is owned and managed by a cloud service provider and is located off-premise (i.e., in the cloud service provider's region of control). This means that customer data is outside its control and could potentially be granted to untrusted parties.

Storage services based on public clouds such as Microsoft's Azure storage service and Amazon's S3 provide customers with scalable and dynamic storage. By moving their data to the cloud customers can avoid the costs of building and maintaining a private storage infrastructure, opting instead to pay a service provider as a function of its needs. For most customers, this provides several benefits including availability (i.e., being able to access data from anywhere) and reliability (i.e., not having to worry about backups) at a relatively low cost. While the benefits of using a public cloud infrastructure are clear, it introduces significant security and privacy risks. In fact, it seems that the biggest hurdle to the adoption of cloud storage (and cloud computing in general) is concern over the confidentiality and integrity of data. While, so far, consumers have been willing to trade privacy for the convenience of software services (e.g., for web-based email, calendars, pictures etc…), this is not the case for enterprises and government organizations. This reluctance can be attributed to several factors that range from a desire to protect mission-critical data to regulatory obligations to preserve the confidentiality and integrity of data. The latter can occur when the customer is responsible for keeping personally identifiable information (PII), or medical and financial records. So while cloud storage has enormous promise, unless the issues of confidentiality and integrity are addressed many potential customers will be reluctant to make the move. To address the concerns outlined above and increase the adoption of cloud storage, we argue for designing a virtual private storage service based on new cryptographic techniques. Such a service should aim to achieve the "best of both worlds" by providing the security of a private cloud and the functionality and cost savings of a public cloud. More precisely, such a service should provide (at least): confidentiality: the cloud storage provider does not learn any information about customer data integrity: any unauthorized modification of customer data by the cloud storage provider can be detected by the customer non repudiation: any access to customer data is logged, while retaining the main benefits of a public storage service:

Availability: customer data is accessible from any machine and at all times

Reliability: customer data is reliably backed up

Efficient retrieval: data retrieval times are comparable to a public cloud storage service

Data sharing: customers can share their data with trusted parties.

An important aspect of a cryptographic storage service is that the security properties described above are achieved based on strong cryptographic guarantees as opposed to legal, physical and access control mechanisms. We believe this has several important benefits.

There are number of similar works has been contributed by number of users. A secure data regeneration scheme for cloud storage has been developed which includes a new cryptographic method for secure Proof of Ownership (PoW), based on the joint use of convergent encryption and the Merkle-based Tree, for improving data security in cloud storage systems, providing dynamic sharing between users and ensuring efficient data deduplication. This idea consists in using the Merkle-based Tree over encrypted data, in order to derive a unique identifier of outsourced data. On one hand, this identifier serves to check the availability of the same data in remote cloud servers. On the other hand, it is used to ensure efficient access control in dynamic sharing scenarios.

It propose a solution that provides both security and regeneration and retains benefits offered by each technique. ClouRegen makes use of convergent encryption but prevents the dictionary attacks. The components involved in ClouRegen are: the basic cloud storage provider, a metadata manager and an additional server. The server guarantees data confidentiality even for predictable files. The metadata manager provides a system for key-management and block-level regeneration. Convergent encryption (CE) is a technique that can meet the requirements of two conflicting solutions between regeneration and encryption. In CE, the encryption key is derived and computed based on the data provided. For instance, the key can be the result of the hash of the data segment. However, convergent en- cryption has various well-known weaknesses despite of its suitability. One common vulnerability is the dictionary attack, in which an attacker manages to generate a potential encryption key and, by comparing the two cipher texts, check whether a file has already been stored or not.

A Fast and secure backups with encrypted de-regeneration has also been focused on the security and efficiency of cloud storage, namely that clients outsource their data to cloud storage servers. While cloud storage offers compelling scalability and availability advantages over the current paradigm of “one storing and maintaining its own IT systems and data”, it does not come without security concerns. This has led to studies on cloud storage security and efficiency, which are, however, addressed separately as we discuss below. From the perspective of cloud storage security, there have been two notable notions:

Proof of Data Possession (PDP):

This notion was introduced by Ateniese et al. [2]. It allows a cloud client to verify the

integrity of its data outsourced to the cloud in a very efficient way (i.e., far more efficient than the straightforward solution of downloading the data to the client-end for verification). This notion has been enhanced in various ways [8, 3, 15].

Proof of Retrievability (POR):

This notion was introduced by Juels and Kaliski [10]. Compared with PDP, POR offers an extra property that the client can actually "recover" the data outsourced to the cloud (in the flavor of "knowledge extraction" in zero-knowledge proof). This notion has been enhanced and extended in multiple aspects From the perspective of cloud storage efficiency, deduplication technique has become a common practice of many cloud vendors. In our data integrity protocol the TPA needs to store only a single cryptographic key irrespective of the size of the data file F and two functions which generate a random sequence. The TPA does not store any data with it. The TPA before storing the file at the archive, pre-processes the file and appends some meta data to the file and stores at the archive. At the time of verification the TPA uses this meta data to verify the integrity of the data. It is important to note that our proof of data integrity protocol just checks the integrity of data. But the data can be stored, that is duplicated at redundant data centers to prevent the data loss from natural calamities. If the data has to be modified which involves updation, insertion and deletion of data at the client side ,it requires an additional encryption of fewer data bits. So this scheme supports dynamic behaviour of data.

4. PROBLEM STATEMENT

The cryptographic storage system that enables secure file sharing on un-trusted servers. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

5.SYSTEM MODEL

5.1Cloud Server

A local Cloud which provides priced abundant storage services are been created in this module. The users can upload their data in the cloud. This module can be developed where the cloud storage can be made secure. The cloud is not fully honorable by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to that the cloud server is genuine but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data investigating schemes, but will try to learn the content of the stored data and the identities of

cloud users. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which are supposed to presumably for a fee truly store the data with it and provide it back to the owner whenever required.

The cloud server provides privilege to generate secure multi-owner data sharing scheme called MONA. It denotes that any user in the group can securely share data with others by the cloud. This scheme is able to support dynamic groups comfortably. Respectively, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners but within the group.

5.2 Proxy Server Deployment

Group manager takes charge of followings,

1. Signature Generation

1) Signature Verification

2) Content Regeneration

A proxy agent acts on behalf of the data owner to regenerate authenticators and data blocks on the servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may becomes off-line after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy. Considering that the data owner cannot always stay online in practice, in order to other group content he will be revoked by the cloud server.

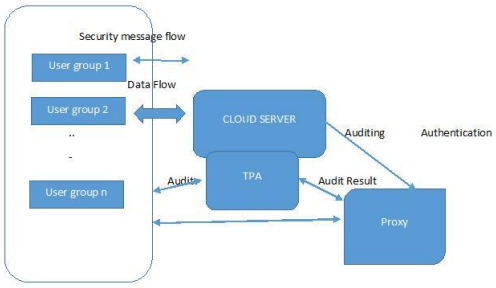

Fig. 1 Cloud Regeneration Architecture

6.MERKLE HASH TREE BASED ARCHIVING:

This technique tries to verify a proof that the data stored by a user at cloud is not modified and thereby the integrity of the data is assured. Cloud archive is not defrauding the owner, if cheating, in this context, means that the storage archive might delete some of the data or may magnify some of the data. While developing proofs for data possession at untrusted cloud storage servers we are often defined by the resources at the cloud server as well as at the client. keep the storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators. It generates signature using OAEP based key delegation which provides unique private and public key for each group registered in the cloud. So the users can access the document provided by its own group only.

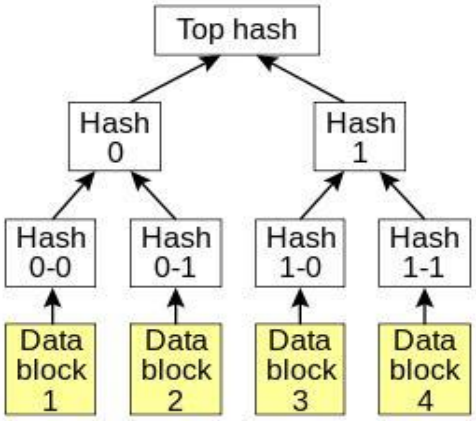

Fig 2 A Merkle Hash Tree

The users can view other groups document using private key of the other groups. If he modifies In this scheme, unlike in the key hash way scheme, only a single key can be used irrespective of the size of the file or the number of files whose retrievability it is want to verify. Also the archive needs to access only a small portion of the file F unlike in the key has scheme which required the annals to process the entire file F for each protocol verification. If the prover had magnify or deleted a substantial allocation of F, then with high probability it will also have suppressed a number of sentinels.

7.CONCLUSION

In this paper, we propose a public investigating scheme for the regenerating-code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. To protect the original data privacy against the TPA, we randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practise, in order to keep the storage available and verifiable after a malicious corruption, we introduce a semi trusted proxy into the system model and provide a

privilege for the proxy to handle the reparation of the coded blocks and authenticators. To better appropriate for the regenerating-code-scenario, we mapping our authenticator based on the BLS signature. This authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure, and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud storage system.

8.REFERENCE

[1] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data regeneration scheme for cloud storage," in *Technical Report*, 2013.

[2] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from regenerate files in a serverless distributed file system." in *ICDCS*, 2002, pp. 617–624.

[3] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-regeneration," in *Proc. of USENIX LISA*, 2010.

[4] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Serveraided encryption for deregenerated storage," in *USENIX Security Symposium*, 2013.

[5] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology: Proceedings of CRYPTO '84*, ser. Lecture Notes in Computer Science, G. R. Blakley and D. Chaum, Eds. Springer-Verlag Berlin/Heidelberg, 1985, vol. 196, pp. 242–268.

[6] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure regeneration with efficient and reliable convergent key management," in *IEEE Transactions on Parallel and Distributed Systems*, 2014, pp. vol. 25(6), include Networking, Cloud Computing, and Data Mining. pp. 1615–1625.

[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman- Peleg, "Proofs of ownership in remote storage systems." in *ACM Conference on Computer and Communications Security*, Y. Chen, G. Danezis, and V. Shmatikov, Eds. ACM, 2011, pp. 491–500.

[8] C. Liu, Y. Gu, L. Sun, B. Yan, and D. Wang, "R-admad: High reliability provision for large-scale de-regeneration archival storage systems," in *Proceedings of the 23rd international conference on Supercomputing*, pp. 370–379.

[9] M. Li, C. Qin, P. P. C. Lee, and J. Li, "Convergent dispersal: Toward storage-efficient security in a cloud-of-clouds," in *The 6th USENIX Workshop on Hot Topics in Storage and File Systems*, 2014.

[10] J. S. Plank and L. Xu, "Optimizing Cauchy Reed-solomon Codes for fault-tolerant network storage applications," in *NCA-06: 5th IEEE International Symposium on Network Computing Applications*, Cambridge, MA, July 2006.

[11] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: Regeneration in cloud.

[12] J. S. Plank, S. Simmerman, and C. D. Schuman, "Jerasure: A library in C/C++ facilitating erasure coding for storage applications - Version 1.2," University of Tennessee, Tech. Rep. CS-08-627, August 2008.

[13] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *Journal of the ACM*, vol. 36, no. 2, pp. 335–348, Apr. 1989.
[14] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

AUTHORS BIOGRAPHY

Ms. S.Jeevitha Pursuing ME(CSE) degree in Shree Venkateshwara Hi-Tech Engineering College, Erode, India in 2014-2016 and B.E (CSE) degree from the Sasurie College of Engineering, Tirupur ,India in 2010-2014 .She is a Member of Computer Society of India (CSI). She published 1 National Conferences, 4 Workshops. Her research interests include Networking, Cloud Computing, and DataMining.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem , India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.

Ms. C.Janani Pursuing ME (CSE) degree in Shree Venkateshwara Hi-Tech Engineering College, Erode, India in 2014-2016 and B.Tech (IT) degree from the Hindusthan College of Engineering and Technology, Coimbatore, India in 2010-2014. She is a Member of Computer Society of India (CSI). She published 1 National Conferences, 4 Workshops. Her research interests include Networking, Cloud Computing, and Data Mining.