International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey on Cloud Storage Privacy Preserving Public Auditing for Regenerating Code

Sonali Bhausaheb Chemate[1], Mansi Bhonsle[2]

[1]M E Student, G. H. Raisoni College of Engineering and Management, Ahmednagar, 414001, India

[2]Associate Professor, G. H. Raisoni College of Engineering and Management, Wagholi, Pune 411015, India

Abstract: ***Cloud is a new way to store large amount of data. In cloud computing, data owners host their data on cloud servers and users can access the data from cloud servers. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. But because of the large amount of data on the cloud it increases privacy challenges against data loss and hacking. For earlier it uses regenerating code while providing fault tolerance against data loss. But because of the fault tolerance the data owner need to always stay online to verify the user data. But challenges are providing integrity of the data. Public audit ability for cloud storage allows users to ask third party auditor (TPA) to check the integrity of the data. Here it analyzes various issues and challenges regarding the data privacy when the data is stored on the cloud. In the various papers it gives various techniques regarding privacy preserving public auditing using the key signature process of secured cloud storage***.

Keywords: Cloud computing, privacy preserving, public auditing, Cloud storage provider, Data integrity

1. Introduction

Cloud computing is very important in case of information storage on the cloud. It allows data owners to move data from their local computing system on the cloud. Cloud storage gain more popularity due to their elasticity and low maintenance cost. Security problem arise when the data outsource through the third party cloud storage. As more and more data owner start to store data on the cloud this is because they introduce new security challenges. This is because data loss could happen.

A. Cloud storage

Cloud is a model of data storage where the digital data is stored. Cloud storage providers are responsible for keeping the data available and accessible. There are three main cloud storage models:

- Public cloud: Storage services, such as Amazon's Simple Service, provide a multi-tenant storage environment that's most suitable for unstructured data.
- Private Cloud: Storage services provide a dedicated environment protected behind an organization's firewall. Private clouds are appropriate for users who need customization and more control over their data.
- Hybrid cloud: Storage is a combination of the other two models that includes at least one private cloud and one public cloud infrastructure. An organization might, for example, store actively used and structured data in a private cloud and unstructured and archival data in a public cloud [1].

Cloud computing has three service models. They are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages. Cloud computing is delivery of computing services over the internet. Cloud services allow individuals and business to use software and hardware that are managed by third parties at remote locations. Cloud computing provides a shared pool of resources, including data storage space, network, computer processing power, and specialized corporate and user applications.

B. Security Issues in Cloud Computing

- Privacy and Security: Regarding authentication to the user
- Reliability and Availability
- Data Privacy: maintaining accuracy and privacy of the data.[1,3]

C. System Model

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server/ cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data.

TPA is reliable and independent. TPA should regularly check the data integrity and availability at frequent time intervals. TPA should be allowed for organizing, managing, and maintaining the outsourced data instead of data owners. It also makes sure that it does not trouble data owners. To support this Cloud Storage Provider should allow and maintain the TPA. TPA must provide trust and security. TPA should not allow malicious attacks, and should prevent unauthorized access that may include members within the clouds. For better security TPA can be allowed under a trusted third party (TTP). This mechanism ensures good performance of audit services and allows maximum access transparency to the data owner.[1,2]

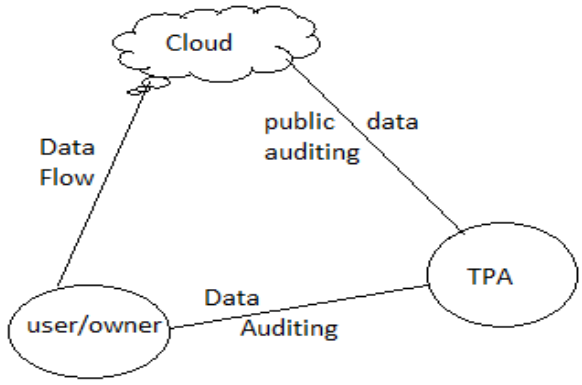

Figure 1: proposed system mode

2. Related work

[1] Arun Kumar K, Gnanadeepa S. Hepzibha John, Janani G. K, "*Survey on Security and Privacy Preserving Public Auditing for Content Storage in Cloud Environment"* Cloud computing it means sharing various resources over internet. User can share and store data remotely. Cloud storage mainly important in terms of local storage without worrying about the need to verify its integrity. But main challenge in data integrity. Public auditing allows third part authenticator to verify the user data to check the data integrity. Public auditing allows third party authenticator to verify the user data to check the data integrity. This paper discuss various issues regarding privacy while cloud data storage. In this paper it present methods provide various solution to preserve privacy of data and also allow auditing on data to check integrity of the data.

[2] Henry C.H. Chen and Patrick P.C. Lee, "*Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud storage: Theory and Implementation*", 2014: For protecting outsourced data against corruption it adding fault tolerance along with efficient data integrity checking but it is becoming critical. During the failure recovery regenerating code provide fault tolerance. In this paper we study the problem of remotely checking the integrity of regenerating coded data against corruption under real life cloud storage setting. For that we design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving its intrinsic properties of fault tolerance and repair- traffic saving. DIP scheme enables general or malicious corruptions. Here DIP scheme is design and implement and further analyse the security strengths of our DIP scheme via mathematical models.

[3] Kan Yang, Xiaohua Jia, "*An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 2012:* In cloud computing data owner host their data on cloud server and user can access their data from cloud server. Due to outsourcing this new paradigm increases the new security challenges which require checking the data integrity in cloud storage. Some techniques are available for static data storage but for dynamic data storage an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper design an auditing framework for cloud storage system and proposes an efficient privacy preserving auditing protocol. This auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. Also this auditing protocol support for both multiple owners and multiple clouds, without using any trusted organizer. This paper implements secure dynamic auditing protocol.

[4] Yan Zhu, Hongxin Hu, Gail-Joon Ahn and Mengyang Yu, "*Cooperative provable Data Possession for Integrity Verification in Multicloud Storage*", 2012: Provable data possession (PDP) is the technique for ensuring the integrity of the data storage. Construction of the PDP scheme for distributed data storage to support scalability of service and data migration, which cooperatively store and maintains client data on multiple cloud service. Here proposed cooperative PDP scheme based on homomorphic verifiable response and hash index hierarchy based on homomorphic verifiable response and index hierarchy, here proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers.

[5] Kevin D.Bowers, Ari Juels, Alina Oprea, "HAIL: A High- Availability and Integrity Layer for Cloud Storage" : In this paper it introduce the High Availability and Integrity Layer (HAIL) for distributed cryptographic system that permits a set of server that permits a set of server that prove to client that stored file is intact and retrievable. HAIL cryptographically verifies and reactively reallocates file shares. This paper shows how HAIL improves on security and efficiency of existing tools, like Proofs of Retrievability (POR) deployed on individual servers.

[6] Ari Juels Burton S. Kaliski Jr. "PORs: Proofs of Retrievability for Large Files", in this paper it define and explore proof of irretrievability (PORs). It enables an backup service to produce concise proof that user can retrieve a target file. A POR may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file F. PORs as an important tool for semi trusted online archives. Cryptographic technique helps to ensure integrity and privacy of the file they retrieve. The goal of POR is to accomplish these checks without users having to download the files themselves. A POR can also provide quality of service guarantees, i.e. show that a file is retrievable within a certain time bound.

[7] ANUPRIYA A.S. ANANTHI, Dr. S. KARTIK, "TPA Based Cloud Storage Security Techniques", cloud computing is the reduces the business investment and satisfy the client need in terms of internet. User can store data and retrieve data from cloud when it is needed. But there is no guarantee of the data security and not changed by the third party auditor. Users should be able to assist the TPA to overcome the integrity problems in cloud. Here it presents various methods of securing the TPA. The Third Party Auditing allows to save the time and computation resources with reduced online burden of users.

[8] Boyang Wang, Baochum Li, and Hui Li, "Oruta: Privacy Preserving Public Auditing for Shared Data in the Cloud" Cloud is the common place to store data but it is also store along with multiple user because of that it is

big challenge regarding security of the data to be store. Here in this paper it presents the first privacy preserving mechanism that allows public auditing of the shared data. In this paper it presents the identity of the shared data that is kept private from third party auditor who publicly verify the integrity of the shared data without retrieving the entire file. Here TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy.

[9] Giuseppe Ateniese, Randal Burns, Reza Curtmola Joseph Herring, Lea Kissner ,Zachary Peterson,Dawn Song," Provable Data Possession at Untrusted Stores", In this paper it provable data possession techniques that allows user to verify that data without retrieving the original file. It have constant amount of metadata to verify the proof. Transmitting constant amount of data it minimizes the network communication.

[10] Reza Curtmola, Osama khan, Randal Burns, Giuseppe Ateniese, "MR-PDP: Multiple Replica Provable Data Possession", in this paper it represents a storage system replication that increases availability and durability of the data. This provides no strong evidence that multiple copies of the data are actually stored. It presents MR-PDP techniques that present t replicas to verify the challenges. This unique replica can produce at t unique time and that system uses t time to store the t unique replica. It presents t replica that is much more efficient that using single replica.

[11] Monjur Ahmed and Mohammad Ashraf Hossian," Cloud Computing and Security Issues in the Cloud" In this paper it represents the various security issues that occurs in the cloud computing environment. There are various issues related to the cloud in the different areas. This paper presents review on the cloud computing concept as well as security issues inherent within the context on cloud computing and cloud environment.

[12] V anto Vins, S Umamageswari, P Saranya, " A survey on Regenerating code", In this paper it represent that remote system are connected through the internet. Also we can outsource software, infrastructure and data from the cloud environment. Once we outsource the data it has chances to corrupt the data or hacked the data. When the repair traffic is high then the fault tolerance is low. To improve the efficiency and the repair traffic it will be using the regenerating code. In this paper it represents various regenerating code that is evolved from time to time.

[13] Dr. G.K.Kamalam, B.Neka, E Jamunadevi, "Secure and Efficient Privacy Preserving Public Auditing Scheme for Cloud Storage", in this paper it represents cloud is a common place to store and access data. For cloud security effective and secure method are needed to privacy and integrity of the data. This paper provides privacy preserving public auditing scheme that support public auditing and privacy support. This paper concentrated on improving the security mechanism of cloud storage service.

[14] Jyoti R Bolannavar, "Privacy Preserving Public Auditing using TPA for secure cloud storage", in this paper it represents that cloud storage remotely store the data and enjoying that data. When the data is locally store then there is no need to check integrity of that data. But when need to check the integrity of the data then it will be need to check the public auditing and that is done by using the TPA. It proposed secure cloud storage system supporting privacy preserving public auditing. Also it extends that TPA can perform audits for multiple user simultaneously.

[15] R. Arokia Paul Rajan, S. Shanmugapriyaa, "Evolution of Cloud storage as cloud computing Infrastructure service", in this paper it represents three service model that are available for cloud storage. Cloud storage is mainly related to new things but without the fundamental of the storage piece. This paper represents various cloud storage which cover the key technology in the cloud storage. Also different types of cloud service and the cloud storage and the advantages and challenges of the cloud storage.

[16] Hamed Alizadeh and Jaber Karimpour, "Analysis of quality of service in cloud storage system", in this paper it represent the cloud storage methods and also represents the quality of service method. Cloud storage is a system composed of multiple computers that cooperate to optionally store lots of file. Due to failure in the file server in that case there is no guarantee of the getting response to the user. In this paper here analyse how to apply quality of the service in cloud storage system to improve the fault tolerance and availability.

[17] Subeg Singh, Richa Sapra, "Secure Replication Management in cloud storage", in this paper it represents that cloud is new way of economically and efficient storage system is less secure because data remain store in the single data mart. Data loss occurs in case of hacking and server failure. In this paper it represent the secure replication approach that encrypt and replicate data in the distribute data mart storage system. This approach involves the replication, encryption and data storage system.

[18] Neethu Mariam Joseph, Ester Daniel, N.A. Vasanthi, "A survey on Privacy Preserving Methods for storage in cloud computing", in this paper it represents when the data are store on the cloud then it has many security issues related to that. This paper represents various security issues associated with privacy while storing the data by third party service provider. This paper is regards of one of the key issues privacy that occur in the context of cloud computing and analyse the various work being done to solve the security issues in the privacy.

[19] Salve Bhagyashri, Prof Y. B. Gurav, "A survey on privacy preserving techniques for secure cloud storage", in this paper it represents when the data is remotely stores on the cloud then there is no need for the auditing but when the data is store on the cloud by multiple user then there is need to check the integrity of the data by using TPA. In this paper it gives various issue of privacy preserving while storing the data to the cloud storage during the TPA auditing. In this paper it analyse the various techniques to analyse the issue and to provide privacy and security of the data in the cloud.

[20] Tejashree Paigude, Prof T.A Chavan , "A survey on privacy preserving public auditing for data storage security", in this paper it represent on the cloud we can store the data without worrying about the correctness and the integrity of the data. User can upload the data on the cloud and can be access that data anytime and anywhere. User no needs to worry about the maintence of the data.

In this paper it presents the new innovative idea about of privacy preserving public auditing. It also support data dynamics where user can perform various operations like insert, update, delete and auditing.

3. Conclusions and future work

In this paper we study the different papers regarding privacy preserving public auditing for regenerating code based cloud storage. Here in the review papers it gives idea regarding privacy of the data in terms of encryption by using secrete key it gives authentication but for authentication data owner need to stay online. Also we studied the system model of privacy preserving public auditing for regenerating code based cloud storage.

In the future work when the data owner not available/online then in that case by using TPA and proxy server it gives authentication to the user so that it reduce the stress of the owner.

4. Acknowledgment

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future. Also I would like to thank my guide Prof. Mansi Bhonsle for her valuable guidance.

References

[1] Arun Kumar.K, Gnanadeepa.S, Hepzibha John, Janani.G.K, "*Survey on Security and Privacy Preserving Public Auditing for Content Storage in Cloud Environment*", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015

[2] H. C. H. Chen and P. P. C. Lee, "Enabling data integrity protection inregenerating-coding- based cloud storage: Theory and implementation,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 407–416, Feb 2014

[3] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*,vol. 24, no. 9, pp. 1717–1726, Sep. 2013

[4] Y. Zhu, H. Hu, G.-J.Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Trans.Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012.*.

[5] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability andintegrity layer for cloud storage," in *Proc. 16th ACM Conf. ComputCommun. Secur.*, 2009, pp. 187–198.

[6] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability forlarge files," in *Proc. 14th ACM Conf. Comput. Commun.Secur*, 2007,pp. 584–597.

[7] ANUPRIYA.A.S, ANANTHI, Dr. S KARTHIK "TPA BASED CLOUD STORAGE SECURITY TECHNIQUES", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012

[8] Boyang Wang, Baochun Li, and Hui Li, Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Transaction

[9] G. Ateniese*et al.*, "Provable data possession at untrusted stores," in*Proc.14th ACM Conf. Comput.Commun.Secur. (CCS)*, New York, NY,USA, 2007, pp. 598–609

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in *Proc. 28th Int. Conf.Distrib. Comput. Syst. (ICDCS), Jun. 2008, pp. 411–420.*

[11] Monjur Ahmed and Mohammad Ashraf Hossian, "Cloud Computing and Security Issues in the Cloud", International Journal of network security & Its Application.

[12] V anto Vins, S. Umamageswari, P. Saranya, "A survey on Regenerating code", International Journal of Scientific and Research Publication, November 2014

[13] Dr. G.K. Kamalam, B. Neka, E. Jamunadevi, "Secure and Efficient Privacy Preserving Public auditing scheme for cloud Storage", International Journal of Computer Network and Security,2015

[14] Jyoti R Bolannavar, "privacy preserving public auditing using TPA for secure cloud storage.", International Journal of Scientific Engineering and research

[15] R.Arokia Paul Rajan, S. Shanmugapriyaa, "Evolution of cloud storage as cloud computing infrastructure service ", IOSR journal of computer engineering.

[16] Hamed Alizadeh and Jaber Karimpour , "Analysis of quality of service in cloud storage system", International journal in foundations of computer science and technology.

[17] Subeg Singh, Richa Sapra, "Secure Replication Management in Cloud Storage", International Journal of Emerging Trends and Technology in Computer Science.

[18] Neethu Mariam Joseph, Ester Daniel, N.A. Vasanthi, "A survey on Privacy Preserving Methods for storage in cloud computing", Amrita International Conference of women in computing

[19] Salve Bhagyashri, Prof Y.B. Gurav, "A survey on privacy preserving Techniques for secure cloud storage", International Journal of Computer science and Mobile computing , feb 2014

[20] Tejashree Paigude, Prof T.A. Chavan, "A survey on privacy preserving public auditing for data storage security", International journal of computer trends and Technology, 2013