A survey on Privacy Data Access control with minimize storage cost in cloud

Vitthal s. gutte
CSE Dept. Amity University Mumbai
Mumbai Pune expressway Panvel
410206*vitthalgutte2014@gmail.com*

Dr. Kamachi Iyyer
CSE Dept. Amity University Mumbai
Mumbai Pune expressway Panvel 410206
Kiyer@mum.amity.edu

***Abstract*—In the new area of research and innovation Cloud Computing is the big environment to work for storage collection and privacy to that data. As the content of advantage of cloud computing and storage technology, large-scale databases are generally exponentially generated today. With the advancement of digital media and storage technology, large-scale digital content datasets are being exponentially generated today, For example image dataset categories such as medical images, satellite images each dataset contains thousands of images for further processing or study. Along with such fast-growing trend to image storage management systems to cloud it still faces a number of fundamental and critical challenges, among which storage space and security is the top concern. The cost for storing data can be reduce with innovative method to get maximum benefit in the cost.**

***Keywords*— Cloud Computing, security, database**

I. Introduction

In the cloud security concern shows more importance .In the storing your personal data on public cloud; data encryption is a great way to discourage people from accessing unauthorized data.

If you plan to store your data on the public cloud security key will identify them as your own work and discourage people from copy the data or claiming them. As their own and in case of cloud storage it makes it very difficult for maintaining storage space and also security for that matter. Cloud computing is a technology that keep data and its application by using internet and central remote servers. This is new computing paradigm with the implications for greater flexibility and availability with the minimum cost. Because of this, cloud computing has been receiving a good attention from many people with different work areas. When using the storage services offered by Cloud service providers it is very important to secure information that enters the cloud and protecting the privacy associated with it. Thus requires deeper security into the cloud's infrastructure. As privacy issues are sure to be central to user concerns about the adoption of Cloud computing, building such protections into the design and operation of the Cloud is vital to the future success of this new networking paradigm[1].

The use control for the cloud environment is more important as we consider the security aspects.. The deployment and running of cloud services requires high skill jobs and people but the unavailability of highly skillful person is a serious issue from the point of view of information security. Unauthorized Secondary Usage: The risk of users use of data either stored or processed in the cloud is always be present. The authorized secondary usage of any user's data by the service provider to gain the revenue is part of standard business model. The data could be used in a way which is always unacceptable to the user. So that it is necessary for the cloud service providers and also the customers to enter into a legally binding agreement which will help explicitly mentions as to how and up to what extent the data of a customer could be used for purpose. This enhances the trust between the customers and the cloud service providers. Complexity of Regulatory Compliance: complicates the compliance issue is the presence of multiple copies of same data in the cloud, and also each of these copies can be managed by different entities in the environment. The main properties which make compliance difficult are as follows Data Proliferation: This is one of the advancing feature of cloud computing in which to ensure the availability of some data in system. The cloud providers replicate that data in multiple locations in area same area[4]. Dynamic Provisioning: The problems mainly related to outsourcing the data which cloud be computing environment faces are mostly similar to that in traditional outsourcing. But the dynamic nature of cloud environment makes many of the existing provisions which address these issues in static environment outdated. Trans border Data Flow: The privacy laws and also data protection regulation restricts the flow of private data outside the national borders and fences, restrict not only the physical transfer of data but also remote access to the data in environment.[5] In the concern of maximum cost and minimum cost cloud should be more active and less payable . The framework for every aspect is different in the cloud privacy more concern relates with different attacks protecting from concern system [7].

II. Leturature SURVEY

A [1]

Challenge in Paper:

The author has to ensure the data correction, storage correction and also error localization, storage management in cloud.

Gap Analysis:

Author explain that the system to ensure data correction, storage and error localization but Anyone can intentionally access or modify the data files as long as they are internally consistent. For that author does not used any encryption scheme.

Statement of Aims and Objectives:

Author has extensive study, effective and also flexible distributed scheme with explicitly dynamic data support to confirm the correctness of users' data in the cloud. The data correcting code in file distribution preparation to provide redundancy and guarantee of data dependability. The system also provides drastically reduce the communication and storage overhead with compare to the traditionally replication based file distribution techniques.

Methodology used:

Author used homomorphic token with distributed verification of erasure-coded data. Proposed system is highly efficient also the resilient against malicious data modification attack server colluding attacks and Byzantine failure in the system.

The method achieves the storage correctness insurance as well data error localization in different parameters.

B[2]

Challenge in Paper:

Correctness maintain challenge

Authors should have a design the system in a way that it will be highly efficient and also resilient against the attacks like malicious data modification attacks also black hole attacks, server colluding attacks and also Byzantine failure.

Gap Analysis:

Analysis about the method shows that system is built to maintain data correctness and proves that system is provably secure for data but User's files are not encrypted on some open source cloud storage systems.

Statement of Aims and Objectives:

In this paper author explain about Cloud storage and process to remotely storage of data and the on-demand high quality cloud computing applications without the burden of local hardware and also software management and explained the benefits of the same on the system.

Methodology used:

In this paper author proposed a flexible or movable distributed storage integrity auditing mechanism, which utilizes the homomorphic token and also distributed erasure- coded data. Authors design shows the system in a way that allows users to audit the cloud storage with very lightweight communication between process and computation cost. Authors basic focus on the correctness of the data in cloud. Proposed system is highly efficient and resilient against malicious attacks such as data modification attack, server colluding attacks and also Byzantine failure attacks.

C[3]

Challenge in Paper:

The author has to provide and ensure the secure the specific data and also to built highly efficient architecture. Also to allows batch processing during auditing process.

Gap Analysis:

Author put the analysis on system and proves that system is provably secure but User's files are not encrypted on some open source like cloud storage systems.

Statement of Aims and Objectives:

In this paper, author mainly focus on eliminating the burden of cloud user from the tedious an more difficult and possibly the expensive auditing tasks .Author proposed a privacy-preserving public auditing system to data storage security in cloud computing and also prevent outsourced data miss use or leak. Method performs multiple auditing tasks in a batch manner to get better efficiency. Author also used Amazon EC2 cloud for demonstration.

Methodology used:

Author used the homomorphic linear authenticator and random masking techniques to guarantee that the TPA would not learn any knowledge about data content stored on the cloud server. At last author performed an extensive analysis which shows that their proposed and explained schemes are provably secure and highly efficient

[4]

Challenge in Paper:

The author has to supports data dynamic operations Also to support batch auditing for multiple owners as well as multiple cloud systems, without using any trusted organizer in the environment.

Statement of Aims and Objectives:

Author studies about the data owners and data consumers and their access privileges and basic security challenges that comes with cloud computing, which have the needs an independent auditing service to check the data integrity in the cloud.

Author also told about some existing remote integrity checking methods which can only serve for static archive data. Existing methods of data integrity checking does not suffice existing cloud security needs because the data in the cloud can be dynamically updated. So that author proposed an efficient and secure dynamic auditing protocol.

Methodology used:

In proposed system authors explained their own auditing protocol and designed an auditing framework for cloud storage systems and also propose an efficient and privacy- preserving auditing protocol after that they extend their auditing protocol which support to data dynamic operations and also further extend proposed auditing protocol to support the batch auditing for both multiple clouds as well as multiple owners, without using any trusted organizer in system and this is more efficient than other previous work .

Gap Analysis: Proposed method of the paper provides consistent place to save valuable data and documents but owner's files are not encrypted on open source cloud storage systems.

[5]

Challenge in Paper:

Provide secure outsourcing for the image with the new reconstruction in the cloud domain.

Gap Analysis:

Author explain that the system to provide more security with image reconstruction but anyone can damage system security control with modified data. In long term keep the data more secure is not the guarantee.

Statement of Aims and Objectives:

The OIRS used in the paper for distributed verification of reconstructed images .This method is more secure with framework. It protect from different attack such as malicious.

Methodology used:

In this paper author proposed an outsourced image recovery service (OIRS) a new concept which exploits different domains. In the same time different technologies for more secure and efficiently working design provides service flow .The method provides to stop different over heads in the domain of security parameters in regular use.

III. EXISTING SYSTEM

1. The first thing is traditional cryptographic with different primitives for the security and protect data from violating the content to avoid loss control with the system. User’s direct control is there with the system where data can be hammered at any moment in the specific area. Directly related concepts on security having more security problems with different approach .Even the correctness of data having a big challenge in recent areas.
2. Second and important is just third party data ware house where most of the time different options perform on the data can have many options. In the process of ensuring correctness of data where the system is dynamic and more parameters are there.

IV. PROPOSED SYSTEM

We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user and user’s data in the cloud. We rely on erasure correcting code in the file storage preparation to provide redundancies and guarantee the data dependability. Our goal is to build up a repository to facilitate the data integration and sharing across cloud along with preservation of data confidentiality. For this we will be using an effective chuck generation technique to provide data security on data storage.

For storage management we simply storing the compressed images rather than the actual image which can help save the storage cost as much as 50%. But while compressing the image we have to maintain the quality of that image, Understanding these benefits of compressed system is pivotal, because it would allow us to explore new possibilities of establishing secure and privacy-assured image service cloud computing, which aims to take security, complexity, and efficiency into consideration from the very beginning of the service .

V. cONCLUSION

The system gives more correctness of data with more security. While storing the data on cloud concern of cost is minimized while having the perfect data control with different algorithmic strategies. The data integrity provided by The third party auditor with data confidentiality in different types of documents. .

REFERENCES

[1] Cong Wang, Qian Wang, and KuiRen “Ensuring Data Storage Security in Cloud Computing” Quality of Service, 2009. IWQoS. 17th International Workshop on ISSN 1548-615X.

[2] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE.

[3] Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member,IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2,FEBRUARY 2013

[4] An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013.

[5] B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revoation in the Cloud,” In the proceeding IEEE INFOCOM 2013, pp. 2904–2912 , 2013.

[6] Sarvan ,ashutosh “Data Integrity Proofs in Cloud Storage Sravan Kumar R Software Engineering and Technolog” COMSNET 4-8 JAN 2011

[7] Smitha Sundareswaran, Anna C. Squicciarini “Ensuring Distributed Accountability for Data Sharing in the Cloud ” IEEE Transactions on Dependable and Secure Computing , Volume: 9, Issue: 4, July-Aug. 2012