Privacy preserving technique to secure cloud

Vitthal S. Gutte
Pune University, MIT College of engineering,
Kothrud, Pune 411038, India
vitthalgutte2014@gmail.com

Prof. Priya Deshpande
Pune University, MIT College of engineering,
Kothrud, Pune 411038, India
priyardeshpande@gmail.com

Abstract:

Cloud Computing is the big environment to work for storage collection and privacy to that data.With the advantage of cloud computing and storage technology , large-scale databases are generally exponentially generated today. Storage management systems for the cloud it still faces a number of fundamental, basic and critical challenges, among which storage space and security is generally to the top concern. It helps to ensure the correctness of user and user's data in the environment of cloud, we propose third party authentication system for the cloud. Also for the simplified data storage and secure data acquisition. Finally we will perform security analysis and performance analysis which shows that the proposed scheme is highly efficient for maintaining secure data storage and acquisition.

Keywords -Cloud Computing; Storage technology; security; database; storage management .

I. INTRODUCTION

There is a danger factor in 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 most common issues related to privacy in cloud computing environment are: Lack of User Control: Complete control of user on the data is not possible in the cloud storage, even though both the visibility and control of a user is reduced as soon as the cloud environment is used. Lack of Training and Expertise. 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] All countries having national legislations have restricted such transfers. Litigation: A government may force the cloud service provider to give them the data stored in the cloud and also restrictions fot that. All they have to do is to show the requested data is relevantly to some case for a subpoena. Legal Uncertainty: Legal frameworks have been played very important role in the protection of the personal and sensitive information to any users.[7] The basic concepts of such a legal frameworks are generally technology neutral therefore they would still be applicable on cloud computing environments. Still these frameworks need to be updated in the world. now a days keeping the current and future technologies in consideration[8].

II. LITERATURE SURVEY

A[1]

Challenging Issues :

To 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 and Techniques to be 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

B[2]

Challenging Issues:

To maintain data correctness.

To 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:

Author’s 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 and Techniques to be 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]

Challenging Issues:

To ensure the data correction, storage correction and also error localization, storage management.

Gap Analysis:

Author explain that the system to ensure data correction, storage 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:

In this paper, author proposed an effective and also flexible distributed scheme with explicitly dynamic data support to confirm the correctness of users’ data in the cloud. Author also proposed data correcting code in file distribution preparation to provide redundancy and guarantee about the data dependability which will drastically reduces the communication and storage overhead with compare to the traditionally replication based file distribution techniques.

Methodology and Techniques to be 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.

Proposed system achieves the storage correctness insurance as well data error localization.

D[4]

Challenging Issues:

To supports data dynamic operations.

Also to support batch auditing for multiple owners as well as multiple cloud systems , without using any trusted organizer.

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.

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 and Techniques to be 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.

III. PROPOSED SYSTEM

In this paper, we have proposed an effective and flexible distributed scheme with the explicit dynamic data support to ensure the correctness of the users data in the cloud system. An optional third party authentication, who has the expertise and also authorities that users may not have.It is trusted and able to expose risk of cloud storage services on behalf of the users upon request.

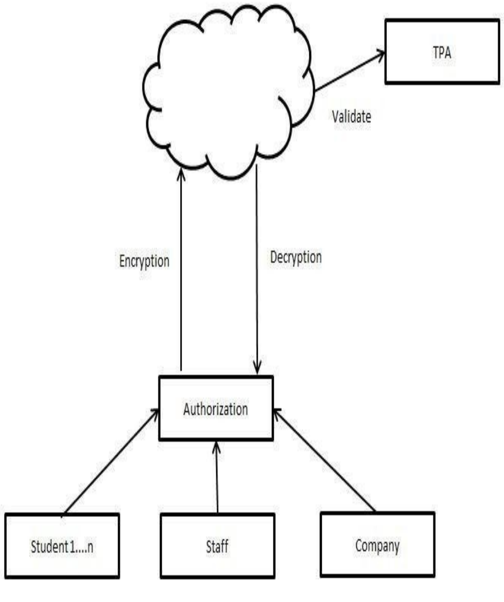

fig 1. Architecture diagram

We propose the method for batch auditing for TPA multiple users,To enable privacy- preserving public auditing for cloud data storage under the proposed model.Our protocol design should achieve the following security and performance guarantees for public auditability to allow the TPA to verify correctness of user's data without retrieving the copy of whole data.We will maintain the storage correctness for ensure that there exist no cheating over cloud servers that can pass the TPA's audit. To maintaining privacy we of cloud have to ensure that TPA cannot derive users data content from the information collected during the auditing process in system.

We also proposes an effective and flexible distributed scheme with the explicitly dynamic data support to ensure the correctness of user and user's data in the cloud. We erasures correcting code in the file storage preparation to provide redundancies and guarantee the data dependency about system. Our goal is to build up a repository to facilitate the data integration and sharing across cloud environment along with preservation of data confidentiality and audit ability. For this we will be using an effective encryption technique which provide data security on data storage.

As shown in fig 1 encrypting the data before storing in cloud can handle the specific confidentiality issues and to ensure correctness of users data in cloud environment. We used TPA, so proposed system provides mainly effective and efficient users data correctness with minimum computation, communication and storage overhead.

In past many years cloud computing has experienced massive growth in the corporate industry, especially as the technology caters to media interoperability and accessibility. Our aim is to build a security service which will be provided with a trusted 3rd party auditor , and would lead to providing only security services.

Main aim to be achieve and provide the security to data in public cloud by focusing on 2 important issues:
1) Integrity
2) Privacy

Detailing it further.

1. To construct Web service system which helps us to provide data integrity verification, provide encryption/decryption of the consumer data.

2. Defining access list for sharing data with security to specific band of individuals.

To construct thin client application which would call this web service before uploading/downloading the data to and from cloud

IV. EXPERIMENTAL SETUP

This project involves the following software and hardware to run the entire application.

Operating System :Windows95/98/2000/XP

Application Server : Tomcat5.0/6.X

Front End : HTML, Java, Jsp

Scripts : JavaScript.

Server side Script : Java Server Pages.

Database : Mysql

Database Connectivity : JDBC

HARDWARE : PROCESSOR - PENTIUM –III

Speed - 1.1 Ghz

RAM - 256 MB (min)

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

V. UML DIAGRAMS

Following figures shows the UML modeling for the proposed system.

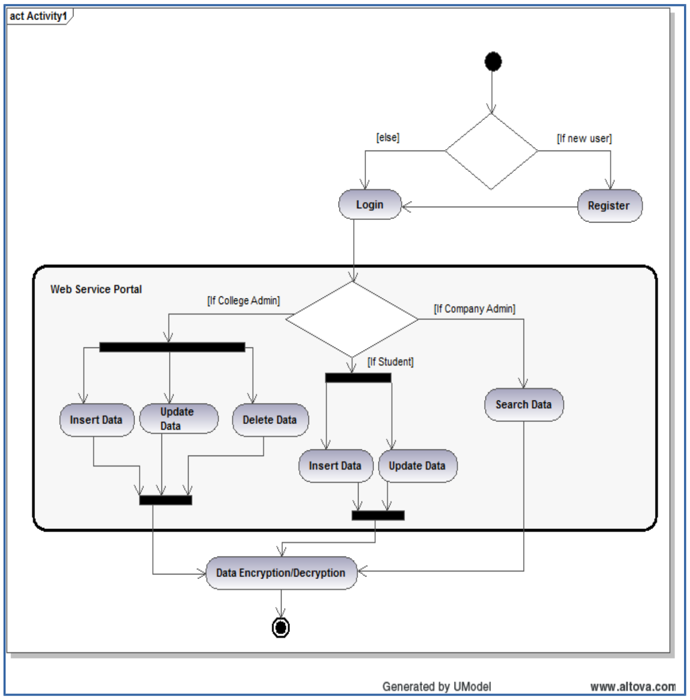

Fig2: activity diagram

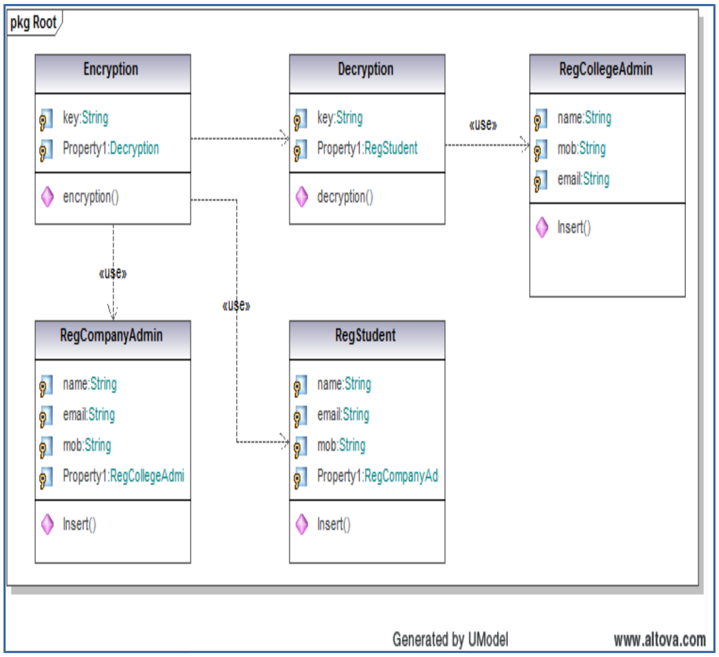

Fig3: class Diagram

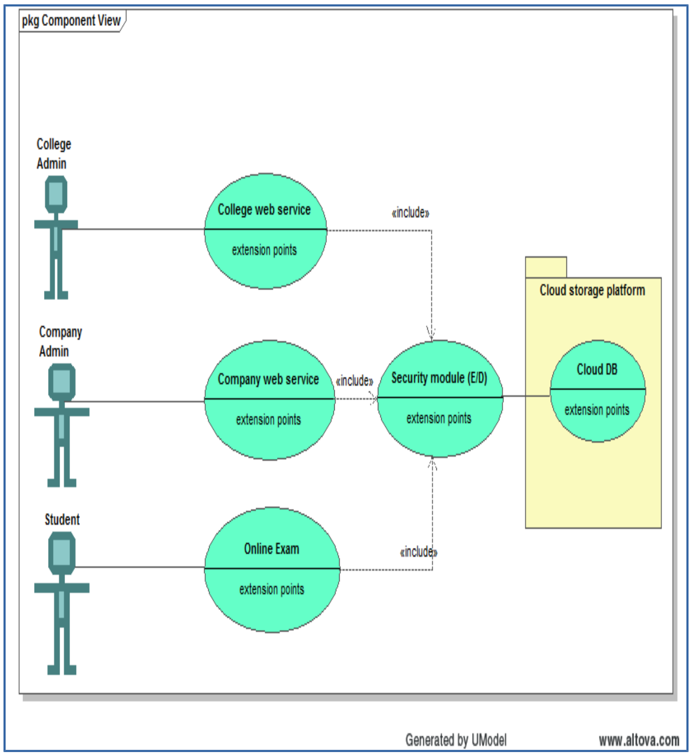

Fig 4 :use case diagram

VI. CONCLUSION

In many systems the main issues is to maintaining the security and also the privacy of confidential data. Cloud stores different types of data for example documents, data sheets, digital media object .It is necessary to give the guarantee about data confidentiality, Data integrity, privacy and auditing are the main issues which examines all the stored data to maintain privacy and integrity of that data and also give data confidentiality.

REFERENCES

[1] 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 .

[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] Ensuring Data Storage Security in Cloud Computing Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology Email: {cwang, qwang, kren}@ece.iit.edu Wenjing Lou Department of ECE Worcester Polytechnic Institute Email: wjlou@ece.wpi.edu

[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 .

[6] Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud CONG WANG1 (Member, IEEE), BINGSHENG ZHANG2 (Member, IEEE), KUI REN2 (Senior Member, IEEE), AND JANET M. ROVEDA3 (Senior Member, IEEE) 1Department of Computer Science, City University of Hong Kong, Hong Kong 2Department of Computer Science and Engineering, The State University of New York at Buffalo, Buffalo, NY 14214 USA 3Department of Electrical and Computer Engineering, University of Arizon at USA (congwang@cityu.edu.hk).

[7]Ensuring Distributed Accountability for Data Sharing in the Cloud Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin .

[8]Data Integrity Proofs in Cloud Storage Sravan Kumar R Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India Email: sravan r@infosys.com Ashutosh Saxena Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India Email: ashutosh saxena01@infosys.com.