



A Survey on Privacy Preserving Technique to Secure Cloud

Vitthal Sadashiv Gutte, Prof. Priya Deshpande
Pune University, MIT College of Engineering, Kothrud,
Pune 411038, Maharashtra, India

Abstract: With the advancement of cloud computing and storage technology, large-scale databases are being exponentially generated today. 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. To ensure the correctness of user and user's data in the cloud, we propose third party authentication system. In addition to simplified data storage and secure data acquisition. Finally we will perform security and performance analysis which shows that the proposed scheme is highly efficient for maintaining secure data storage and acquisition.

Keywords: 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 copying them 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. Cloud computing can considered as a 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.

II. Literature Survey

A. Challenging Issues [1]:

To secure data and also to built highly efficient architecture which allows batch processing during auditing

Gap Analysis:

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

Statement of Aims and Objectives:

In this paper, author focused on eliminating the burden of cloud user from the tedious and possibly expensive auditing task author proposed a privacy-preserving public auditing system for data storage security in cloud computing and also prevent outsourced data leakage. Method also performs multiple auditing tasks in a batch manner for better efficiency. Author used Amazon EC2 cloud for demonstration.

Methodology and Techniques to be Used:

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

B. Challenging Issues [2]:

To maintain data correctness.

To design system in such a way that it will be highly efficient and resilient against attacks like malicious data modification attacks, server colluding attacks and also Byzantine failure.

Gap Analysis:

Author's analysis shows that system is built to maintain data correctness and proves that system is provably secured but User's files are not encrypted on some open source cloud storage systems.

Statement of Aims and Objectives:

In this paper authors described Cloud storage and process to remotely storage of data and the on-demand high quality cloud applications without the burden of local hardware and software management and explained the

benefits of the same.

Methodology and Techniques to be used:

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

C. Challenging Issues [3]:

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

Gap Analysis:

Author proposed that system to ensure data correction, storage correction 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 use any encryption scheme.

Statement of Aims and Objectives:

In this paper, author proposed an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. Author proposed data correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability which drastically reduces the communication and storage overhead as compared to the traditional 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 and resilient against malicious data modification attack server colluding attacks and Byzantine failure. Proposed system not only achieves the storage correctness insurance but also data error localization.

D. Challenging Issues [4]:

To support data dynamic operations.

To support batch auditing for multiple owners as well as multiple clouds, without using any trusted organizer.

Gap Analysis:

Proposed method provide 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 data owners and data consumers and their access privileges and new security challenges that comes with cloud computing, which needs an independent auditing service to check the data integrity in the cloud.

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

Methodology and Techniques to be Used:

In proposed system authors proposed their own auditing protocol and designed an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol and then extend their auditing protocol which support 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.

E. Challenging Issues [5]:

To design a system which supports distributed storage with acceptable cost

Gap Analysis:

Author only proposed distributed storage and it does not ensure data security

Statement of Aims and Objectives:

The main objective was provide applications with explicit knowledge about the properties of the storage resources they desire to use, and, in turn, uses that knowledge to maintain such properties in a manner which limits the costs only to data/state that require them.

Methodology and Techniques to be Used:

In this paper author presents FleCS and its associated abstractions, and explores their utility in supporting diverse and flexible cloud storage services. Through use of storage containers, and their associated attributes, FleCS enables realizations of range of storage services with acceptable costs, include those targeting cross-cloud storage interactions. Authors are continuing to evolve the FleCS prototype and to develop and experiment with realistic applications and use.

III. Proposed Architectures and Methods

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to

ensure the correctness of users data in the cloud. An optional third party authentication, who has expertise and authorities that users may not have, is trusted and is able expose risk of cloud storage services on behalf of the users upon request. We propose batch auditing for TPA for 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 public auditability to allow TPA to verify correctness of user's data without retrieving the copy of whole data. We will maintain storage correctness to ensure that there exist no cheating cloud servers that can pass the TPA's audit. To maintaining privacy we have to ensure that TPA cannot derive users data content from the information collected during the auditing process.

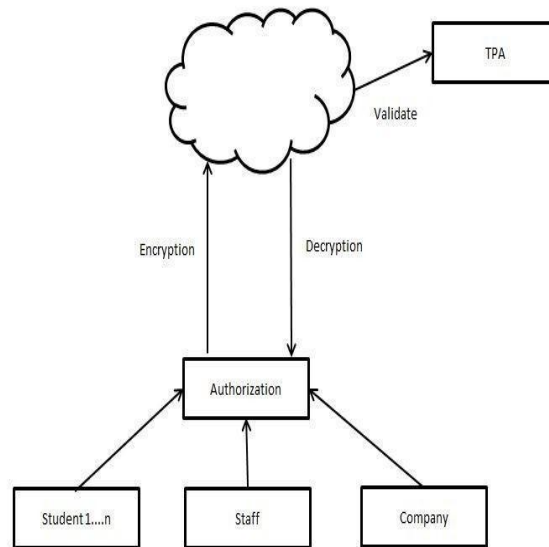


Fig. 3.1 Proposed Architecture

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 erasures 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 encryption technique to provide data security on data storage.

As shown in fig 3.1 encrypting the data before storing in cloud can handle the confidentiality issue and to ensure correctness of users data in cloud we used TPA, so proposed system provides effective and efficient users data correctness with minimum computation, communication and storage overhead.

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

Main aim to be achieved is providing 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 would provide data integrity verification, provide encryption/decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this web service before uploading/downloading the data to and from cloud.

VI. Conclusion

In many organizations the main issues is maintaining the security and privacy of confidential data. Cloud store different types of data for example documents, data sheets, digital media object and it is necessary to give guarantee about data confidentiality. Data integrity, privacy and auditing are the terms which examine all stored data to maintain privacy and integrity of data and 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.
- [5] An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing Syam Kumar, P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University, Puducherry-605014, India.
- [6] Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud CONG WANG (Member, IEEE), BINGSHENG ZHANG (Member, IEEE), KUI REN (Senior Member, IEEE), AND JANET M. ROVEDA (Senior Member, IEEE.) Department of Computer Science, City University of Hong Kong, Hong Kong, Department of Computer Science and Engineering, The State University of New York at Buffalo, Buffalo, NY 14214 USA, Department of Electrical and Computer Engineering, University of Arizona at Tucson, Tucson, AZ 85721 USA.
- [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, Ashutosh Saxena, Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India.
- [9] Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Senior Member, IEEE, Mengyang Yu.
- [10] Cloud Computing Security Issues and Challenges Kuyoro S. O., Department of Computer Science Babcock University Ilishan-Remo, 240001, Nigeria Ibikunle F., Department of Computer Science Covenant University Ota, 240001, Nigeria Awodele O. Department of Computer Science Babcock University Ilishan-Remo, 240001, Nigeria.
- [11] An analysis of security issues for cloud computing Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez.
- [12] Cloud Computing Security Issues, Challenges and Solution International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012) Pradeep Kumar Tiwari, Dr. Bharat Mishra M.phil (CSE) student, Reader in department of physical Science, at Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya Chitrakoot - Satna (M.P.).