

A Survey on Securing Images in Cloud Using Third Party Authentication

Ms. Shubhangi Edake¹
Computer Engineering
Dr. D. Y. Patil School of Engineering
Pune, India
e-mail: shubhangi.edake@gmail.com¹

Prof. Laxmi Madhuri²
Computer Engineering
Dr. D. Y. Patil School of Engineering
Pune, India
e-mail: madhuri.laxmi@dypic.in²

Abstract: With the advancement of digital media and storage technology, large-scale image datasets are being exponentially generated today, 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. To ensure the correctness of user and user's data in the cloud, we propose third party authentication system. In addition to simplified image storage and secure image acquisition, one can also apply compressed encryption for the purpose of storage overhead reduction. Finally we will perform security and performance analysis which shows that the proposed scheme is highly efficient for maintaining storage space and secure data acquisition.

Keywords - Storage technology, security, blog, flexibility, availability

I. INTRODUCTION

There is a danger factor in publishing your digital media online, whether you are publishing it professionally or just putting images up on your personal blog. Creating a watermark, for digital media whether it is images or videos is a great way to discourage people from copying photos that you have on your website or any portal. While still allowing the image to be seen. Creating a watermark and placing it on digital images that you plan to post on the web 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 up data and its application by using internet and central remote servers. Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at minimum cost. Because of this, cloud computing has been receiving a good attention from many people with different work area.

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. RELATED WORK

A. Title: Privacy-Preserving Public Auditing for Secure Cloud Storage

Proposed Method:

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 perform multiple auditing tasks in a batch manner for better efficiency. Author used Amazon EC2 cloud for demonstration.

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.

Advantages:

- 1) Proposed schemes are provably secure and highly efficient.
- 2) Allows batch processing

Disadvantages:

- 1) User's files are not encrypted on proposed open source cloud storage systems.

B. Title: Towards Secure and Dependable Storage Services in Cloud Computing

Proposed Method:

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.

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 focuses on the correctness of the data in cloud. Proposed system is highly is highly efficient and resilient against Byzantine failure, data modification attack and server colluding attacks.

Advantages:

- 1) Data correctness is maintained
- 2) Highly efficient and resilient against Byzantine failure, data modification attack and server colluding attacks.

Disadvantages:

- 1) User's files are not encrypted on some open source cloud storage systems.

C. Title: Ensuring Data Storage Security in Cloud Computing

Proposed Method:

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.

Here also used homomorphic token with distributed verification of erasure-coded data.

Proposed system is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Proposed system not only achieves the storage correctness insurance but also data error localization.

Advantages

- 1) Proposed system ensures data correction, storage correction and also error localization.

Disadvantages:

- 1) 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.

D. Title: An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Proposed method:

In proposed system authors proposed their own auditing protocol, before that 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.

Author first design 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 compatible for batch auditing for both multiple owners and clouds, without using any trusted organizer.

Advantages:

- 1) Proposed method supports data dynamic operations.
- 2) Support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

Disadvantages:

- 2) Proposed method provide consistent place to save valuable data and documents but stored files are not encrypted on cloud storage systems.

E. Title: An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing

Proposed Method:

In this paper, authors first studied the problem of Integrity and Confidentiality of data storage in cloud computing. Authors proposed an efficient and secure protocol using ECC and Sobol sequence.

Proposed scheme satisfies the all security and performance requirements of cloud data storage. Our method also supports public verifiability that enables TPA to verify the integrity of data without retrieving original data from the server and probability detects data corruptions.

The proposed method is mainly suitable for thin users who have less resources and limited computing capability scheme also supports dynamic data operations,

Advantages:

- 1) Provides data integrity
- 2) Supports dynamic data operations

Disadvantages: 1) Proposed system is suitable for users having less resources and limited computing capability.

F.Title: Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

Proposed Method:

In this paper, author proposed a framework called OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. Author mainly focus on secure outsourcing of stored images which exploits techniques from different domains, and aims to take security. Author proposed an architecture that contains image processing methods like compression, encryption and decryption which assures storage redundancy and security.

Advantages:

- 1) Security is well preserved
- 2) Allows storage redundancy

Disadvantages:

- 1) Auditing is not performed

III. 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 examines all stored data to maintain privacy and integrity of data and give data confidentiality.

ACKNOWLEDGMENT

I wish to express my sincere thanks to the guide Prof. Laxmi Madhuri and Head of Department, Prof. Soumitra Das , as well as our principal Dr.S.S.Sonavane, also Grateful thanks to our PG Coordinator Prof. P. M. Agarkar and last but not least, the departmental staff members for their support.

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 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 Arizona at Tucson, Tucson, AZ 85721 USA
CORRESPONDING AUTHOR: C. WANG
(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: sravanr@infosys.com Ashutosh Saxena Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India Email: ashutosh.saxena01@infosys.com
- [9] Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage Yan Zhu, HongxinHu, Gail-Joon Ahn, Senior Member, IEEE, MengyangYu
- [10] Cloud Computing Security Issues and Challenges Kuyoro S. O. afolashadeng@gmail.com Department of Computer Science Babcock University Ilishan-Remo, 240001, Nigeria Ibikunle F. faibikunle2@yahoo.co.uk Department of Computer Science Covenant University Ota, 240001, Nigeria Awodele O. dealealways@yahoo.com 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.)