



Security in Multimedia Cloud Computing

Gowrimol D¹

Lecturer ,Computer Engineering ,Women's Polytechnic College,Thrissur,Kearala,India

Abstract: Cloud computing is a computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing permits the usage of applications without installation. It also allows the access of personal files at any computer through the Internet. Multimedia data is a group of some of the following medium: content, audio, moving image, and film. With the development of Internet multimedia computing has emerged as a technology to generate, edit, process, and search media contents, such as images, video, audio, graphics, and so on. Multimedia cloud computing has the tremendous potential but faces many challenges. A major challenge is the security of the multimedia content in the cloud. In order to keep the user data confidential against untrusted servers, various methods have been proposed. This paper conducts a survey on multimedia storage security solutions in organizations with cloud computing. This purpose of the study is to offer state of the art information to new researchers in this field multimedia cloud security. This paper explores a method which is a combination of roll based access control with advanced encryption algorithm ,signature verification to enhance security when storing text, image ,audio ,video files onto cloud server and OTP verification while accessing data stored in the cloud.

Keywords: cloud security, multimedia, encryption

I. INTRODUCTION

With the fast development of current information technology, electronic publishing, such as the distribution of digitized images and videos, is becoming more and more popular. Digital multimedia content such as images and videos can easily be sent through the Internet to the cloud system. In particular, data access over wireless networks from the media cloud has recently found increased popularity due to the fast growth of wireless multimedia applications. However, multimedia security has become an increasingly major concern for cloud media data access control. It is important to ensure secure and reliable multimedia data transmissions between mobile users and the media cloud. It is reasonable that a cloud system can provide security access control. However, the cloud itself may not be trusted since it is managed by third parties such as cloud service providers. The security can only be guaranteed by contracts between users and cloud service providers. There are some potential risks, such as security attacks or misconduct of the cloud manager. A serious security issue can rise in association with the expanding storage data center of the cloud server, which stores multimedia files of users such as personal photos and videos . Top security concerns of cloud computing are Data loss, Leakage of data, Client's trust, User's authentication, Malicious users handling, Wrong usage of Cloud computing and its services, Hijacking of sessions while accessing data, insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, and service disruption. Therefore enhancing the security for multimedia data storage in a cloud centre is of ultimate importance. It is essential for the cloud storage to be equipped with storage security solutions so that the whole cloud storage system is reliable and trustworthy. Various cloud storage security solutions like bilinear pairing method, access control, symmetric cryptographic algorithm like DES, TDES, AES, Blowfish etc., asymmetric algorithm like RSA have been developed rapidly in recent years, there have not yet seen a widely accepted model for the implementation. Besides the system design, the cloud storage security system should be flexible enough so that it can be improved by new cryptographic algorithms.

1. Literature Review

A number of studies showing the need of security in cloud computing especially for the multimedia content storage and the various proposed techniques to enhance security.

Rongxing et al [1] gave a new security and provenance proposal for data forensics and post examination in cloud computing. Their proposed system provides the privacy and security on secret documents/files that are piled up in the cloud and secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their secure provenance scheme is working on the bilinear pairing method.

La.,Quata Sumter et al. [2] says: The rise in the scope of —cloud computing has brought fear about the Internet



Security and the threat of security in cloud computing is continuously increasing. To assure users that their information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud.

Wenchao et al. [4] in this paper have explored the security properties of secure data sharing among the applications hosted on clouds. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2).

Soren et al [5] in this paper have mentioned that benefits of clouds are shadowed with the security, safety and privacy. In this paper an approach has been presented for analyzing security at client side and server side. Amazon's Elastic Compute Cloud (EC2) has been chosen for this assessment. They have implemented the security analysis model & weigh up it for realistic environments. Security assessment has been implemented in Python and weigh up was calculated on Amazon EC2.

Flavi and Roberto [6] stated that clouds are being targeted increasingly day by day. In this paper integrity protection problem in the clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services has been discussed.

Wenwu Zhu et.al [8] presented the fundamental concept and a framework of multimedia cloud computing. They addressed multimedia cloud computing from multimedia-aware cloud and cloud-aware multimedia perspectives.

Tamleek Ali [10] proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as documents and rich media. They have leveraged the UCON model for enforcing fine-grained continuous usage control constraints on objects residing in the cloud.

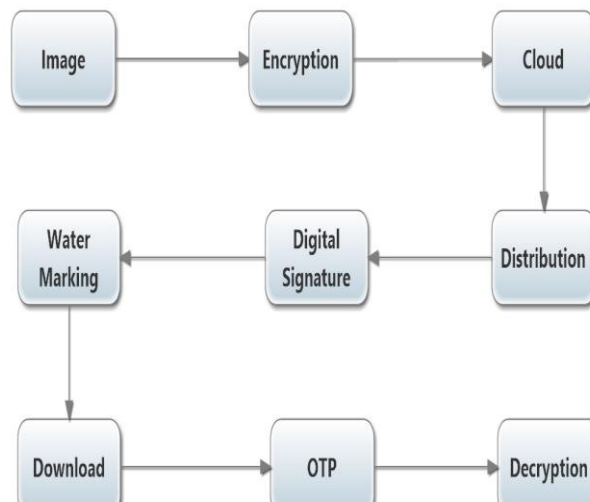
Chun-Ting Huang [12] conduct a depth survey on recent multimedia storage security research activities in association with cloud computing. After an overview of the cloud storage system and its security problem, they focus on four hot research topics. They are data integrity, data confidentiality, access control, and data manipulation in the encrypted domain.

Neha Jain [13] presented a data security system in cloud computing using DES algorithm.

N. Saravanan et.al [14] presented a data security system in cloud computing using RSA algorithm. They have implemented RSA algorithm in google App engine using cloud SQL.

II. PROPOSED SYSTEM

This paper proposes a secure cloud framework which provides security to the cloud environment and to the user. Create a role based access control for admin to assign roles to authenticated user. Only the authenticated users will be able to access data files. This authentication will be checked online on the cloud itself. The images are encrypted and added to the cloud thus the images will be securely stored. The data distribution is provided in the system. Digital signature is generated for each distribution done by the user for same image. The digital signatures are securely embedded using the watermarking method. When attempts are made to download the image that is shared over the cloud, it will ask for the OTP i.e. one time password which will be sent to the corresponding mobile number provided by the user.



III. CONCLUSION

It is required for the cloud storage to be able to provide with storage security solutions so that the whole cloud storage space is consistent and reliable. This paper proposes an efficient framework for providing multimedia data storage in the cloud environment with secure cloud security. A secure architecture is presented where security is provided through a combination of methods like water marking, digital signature and encryption.

ACKNOWLEDGMENT

Mrs.Gowrimol D thanks head of the institution, colleagues and her family members for their support.

REFERENCES

- [1] Rongxing et al, —Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing, ASIACCS.,10, Beijing, China..
- [2] R. La.,Quata Sumter, —Cloud Computing: Security Risk Classification, ACMSE 2010, Oxford, USA
- [3] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009, Feb. 10); “Above the clouds: A Berkeley view of cloud computing” EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009- 8 .
- [4] Wenchao et al, —Towards a Data-centric View of Cloud Security, clouddb2010, Toronto, Canada
- [5] SorenBleikertz et al, —Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds, CCSW 2010, Chicago, USA.
- [6] Flavio Lombardi& Roberto Di Pietro, —Transparent Security for Cloud, SAC.,10 March 22-26, 2010, Sierre, Switzerland.
- [7] Sara Qaisar; “Cloud Computing :Network/Security Threats and Counter Measures, Interdisciplinary Journal of Contemporary Research In Business, Jan 2012,Vol 3, No 9.
- [8] Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li; “Multimedia Cloud Computing” Digital Object Identifier 10.1109/MSP.2011.940269 Date of publication: 19 April 2011.
- [9] Jiann-Liang Chen, Szu-Lin Wu, YanuariusTeofilusLarosa, Pei-Jia Yang, and Yang- Fang Li; “IMS Cloud Computing Architecture for High-Quality Multimedia Applications” 978-1-4577-9538- /11/\$26.00 ©2011 IEEE.
- [10] TameekAli , Mohammad Nauman , Fazl-e- Hadi ,and Fahad bin Muhaya; “On Usage Control of Multimedia Content in and through Cloud Computing Paradigm”.
- [11] Zhang Mian, Zhang Nong; “The Study of Multimedia Data Model Technology Based on Cloud Computing”; 2010 2nd International Conference on Signal Processing Systems (ICSPTS).
- [12] Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo; “Multimedia Storage Security in Cloud Computing: An Overview” 978-1- 4577-1434-4/11/\$26.00©2011IEEE.
- [13] Neha Jain and GurpreetKaur; “Implementing DES Algorithm in Cloud for Data Security” VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
- [14] N. Saravanan, A. Mahendiran, N. VenkataSubramanian;An Implementation of RSA Algorithm in Google Cloud using Cloud SQL” Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, October 01, 2012.

[1] **Mrs.Gowrimol D** ,Now Lecturer in Govt Women’s Polytechnic college,Nedupuzha. She completed BTech in Computer Science & Engineering from Cochin University in 2004 and M.tech in 2007.From 2008-2015; she worked as Lecturer in a few engineering colleges.Her area of interest is graph theory and combinatorics.