Priyanka Gupta, Amandeep Kaur Brar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.2273-2277

An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server

Priyanka Gupta, Amandeep Kaur Brar
(Student, Dept. of ECE, Punjabi University, Patiala, India)
(Prof, Dept. of ECE, Punjabi University, Patiala, India)

Abstract

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. With the development 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 potential for tremendous benefits, but wide scale adoption has a range of challenges like *Multimedia and service heterogeneity, QoS heterogeneity, Network heterogeneity, Device heterogeneity ,Security, Power Consumption* that must be met. But data security and access control is the main challenge when users outsource sensitive data for sharing on cloud servers which is not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, various methods have been proposed in the literature. This paper explores a new method which is a combination of roll based access control with advanced encryption algorithm (a combination of RSA and two fish),signature verification to enhance security when storing text, image ,audio ,video files onto cloud server.

Keywords: cloud, multimedia, RSA, security, storage.

I. INTRODUCTION

1.1 Cloud Computing

Cloud computing is the evolving paradigm which is defined in the term of a virtual infrastructure which can provide shared information and communication technology services, via an internet "cloud," for "multiple external users" through use of the Internet or "large-scale private networks." Cloud computing provides a computer user access to Information Technology (IT) services i.e., applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure. In cloud-based multimedia-computing paradigm, users store and process their multimedia application data in the cloud in a distributed manner, eliminating full installation of the media application software on the users' computer or device and thus alleviating the burden of memory requirement, multimedia software maintenance and upgrade as well as sparing the computation of user devices and saving the battery of mobile phones.

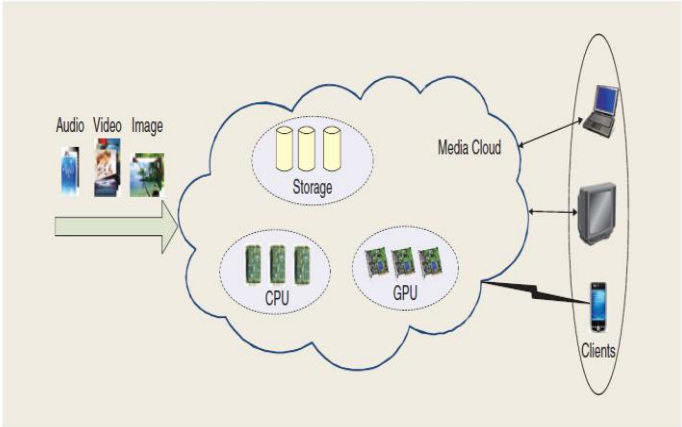

Fig: 1 – Fundamental Concept of Multimedia Cloud Computing

1.2 Challenges in multimedia cloud computing

Multimedia processing in a cloud imposes great challenges. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows.

1) *Multimedia and service heterogeneity*: As there exist different types of multimedia and services, such as voice over IP (VoIP), video conferencing, photo sharing and editing, multimedia streaming, image search, image-based rendering, video transcending and adaptation, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services for millions of users simultaneously.

2) *QoS heterogeneity*: As different multimedia services have different QoS requirements, the cloud shall provide QoS provisioning and support for various types of multimedia services to meet different multimedia QoS requirements.

3) *Network heterogeneity*: As different networks, such as Internet, wireless local area network (LAN), and third generation wireless network, have different network characteristics, such as bandwidth, delay, and jitter, the cloud shall adapt multimedia contents for optimal delivery to various types of devices with different network bandwidths and latencies.

4) *Device heterogeneity*: As different types of devices, such as TVs, personal computers (PCs), and mobile phones, have different capabilities for multimedia processing, the cloud shall have multimedia adaptation capability to fit different types of devices, including CPU, GPU, display, memory, storage, and power.
5) *Security*: As data is stored on the cloud and because of opaqueness nature of cloud, anyone can access the data on the cloud .Therefore security remains an important issue. As a result, security must be imposed on data by using encryption strategies to achieve secured data storage and access.
6) Power Consumption: The expanding scale and density of data centers has made their power consumption an imperative issue.. Moreover, a recent phenomenon has been the astounding increase in multimedia data traffic over the Internet, which in turn is exerting a new burden on the energy resources.

1.3 Cloud Security issues

A serious security issue arises 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 center is of paramount importance.

1.4 Cloud Security Solutions

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.

II. LITERATURE REVIEW

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] in this paper gave a new security and provenance proposal for dataforensics and post examination in cloud computing. According to them their proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed 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 there 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.

III. PROPOSED SCHEME

In this paper we proposed a secure cloud framework .By using this architecture we can provide security to the cloud environment and to the user.

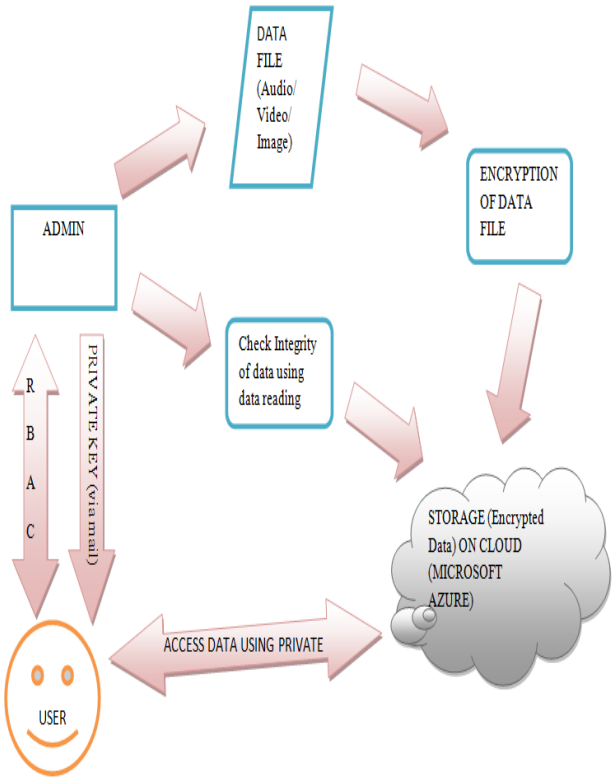

Fig 1:Proposed Scheme

MODULE 1:

- 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 cloud itself.

MODULE 2:

- Storage of data files(audio,video,text,image) with the signature and an encryption algorithm based on combination of RSA and Twofish (to have better security than RSA or Twofish alone) on Microsoft azure cloud.

MODULE 3:

- Whenever an authenticated user tries to access the data file from cloud storage, the private key will be generated on run time for decrypting the file .This private key will be sent to user via mail. To decrypt the data user will be required to enter that private key and the corresponding signature .This will provide enhanced security.

Reasons to choose RSA and Twofish algorithm:-

RSA is basically an asymmetric encryption / decryption algorithm. It was proposed by Rivest, Shamir, and Adleman. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone.

RSA algorithm is one of the best algorithms in the cloud structure system which generates the Private and Public key after the encryption of the content. The private key is to access the content where as the public key is the key through which it gets stored on the cloud architecture. My aim is to enhance the encryption technique, and hence I tried some modification in the existing encryption technique.

What I tried to do: -

I fetched the public key generated from the RSA and applied the Twofish algorithm over that so that the encryption standard may become quite sophisticated to get decrypted in a simpler manner.

Why Twofish?

Twofish is the best choice because of its unique combination of speed ,flexibility and

conservative design. It has the ability to trade off key-setup time for encryption speed.

Tool Used:

Visual Studio **:**It is a platform which provides the way to develop different applications. It is a framework used to develop applications.

Online Tool:

Window Azure: Windows Azure is the cloud service of Microsoft. It comes with easy access and lower price rates It offers a simple, reliable, and powerful platform by which one can host applications and create web applications and services.

4. HOW TO STORE DATA ON AZURE'S CLOUD SERVER?

Steps

- Create an account on windows azure.
- Create database and tables.
- Click on portal and sign in with your username and password .Then click on SQL database,then click on dashboard.After this open your database and click on manage allowed ip address.Then click on add to the allowed ip address and save.
- Again click on SQL database,then open your database and click on dashboard.After this click on manage URL.
- A window will appear in which enter name of your database,username and password and log on.
- Then click on design.
- Open Microsoft Visual studio .Go to file and open your website .View solution explorer.Set login page as start page as only authenticated users are allowed to store data on cloud and run the code.
- A webpage will appear in which select the type of file(text,audio,video,image)you want to upload,write its description,fill the signature and email column and upload the file.Encrypted file will be stored on cloud.
- To download the file enter private key and the signature.

IV. CONCLUSION AND FUTURE PROSPECT

In this paper we proposed an efficient framework to provide data storage in the cloud environment with secure user cloud security. We present a secure three tier architecture in which original file(text,audio,video,image) is stored on local server, the encrypted filename and the description of the original file is stored on cloud server,and to decrypt the file user has to enter private key which is stored in its Gmail account.This will enhance security as if the hacker hacks the local server he will only get original file(not its description),if he hacks the cloud server he will get only the description and not the original file and to decrypt the file he will have to hack the gmail server.

In this paper we taken two most secure algorithms RSA and twofish for encryption and decryption .This security approach make our framework more secure in comparison to the previous .In today's era the demand of cloud is increasing, so the security of the cloud and the user is on the top concern. Our proposed algorithm is helpful for the today's requirement. In future we can provide several comparisons with our approach with result to show the effectiveness of our proposed framework.

6. RESULTS

Various files(audio,video,text,image) have been successfully uploaded and stored in the cloud and accurately downloaded. Graphs have been plotted for download time ,restriction time ,accuracy of file. Download time, restriction time is calculated in seconds and accuracy of file is calculated in percentage.

V. ACKNOWLEDGEMENT

First of all, I would like to thank almighty GOD who has given this wonderful gift of life to us. He is the one who is guiding us in right direction to follow noble path of humanity. I would like to express a deep sense of gratitude and thanks profusely to my supervisor, **Er. Amandeep Kaur Brar** for his able guidance, inspiring & praiseworthy attitude and honest 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-2009-28 .

[4] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada

[5] Soren Bleikertz 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, Yanuarius Teofilus Larosa, Pei-Jia Yang, and Yang-Fang Li; "IMS Cloud Computing Architecture for High-Quality Multimedia Applications" 978-1-4577-9538-2/11/$26.00 ©2011 IEEE.

[10] Tamleek Ali , 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 (ICSPS).

[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 Gurpreet Kaur; "Implementing DES Algorithm in Cloud for Data Security" *VSRD-IJCSIT, Vol. 2 (4), 2012*, 316-321.

[14] N. Saravanan, A. Mahendiran, N. Venkata Subramanian;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.

[15] M. Sudha, Dr.Bandaru Rama Krishna Rao; "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" *International Journal of Computer Applications (0975 – 8887) Volume 12– No.8*, December 2012.

[16] Priyanka Arora, Arun Singh; "Evaluation and Comparison of Security Issues on Cloud Computing Environment" *World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5*, 179-183, 2012.

[17] Yashpalsinh Jadeja, Kirit Modi; "Cloud Computing - Concepts, Architecture and Challenges", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].