Multimedia Content Storage with Hybrid Encryption over Cloud Server

Priyanka Gupta,Amandeep Kaur Brar

Student,Dept. of ECE,Punjabi University,Patiala,Punjab,India

Prof.,Dept. of ECE,Punjabi University,Patiala,Punjab,India

Priyankagarg.gupta@gmail.com

Amandeepbrar123@gmail.com

ABSTRACT

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks ,servers, storage applications and services. In cloud-based multimedia-computing,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.Due to opaqueness nature of cloud ,anyone can access the data in the cloud. Therefore, security is the major limitation in multimedia (personal photos and videos) cloud computing.Various cryptographic algorithms have been proposed in the literature.To enhance security a new system design which is a combination of RBAC, hybrid algorithm(a combination of RSA and AES),signature verification with mail integration has been proposed.

Keywords: AES, Cryptography,Multimedia, RSA,Security.

1.INTRODUCTION

A .Cloud Computing

Cloud computing, a way to increase capacity without investing in new infrastructure, training new personnel, or licensing new software .Cloud computing enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources. In this new cloud based multimedia-computing paradigm, users store and process their multimedia application data in the cloud in a distributed manner. Cloud computing essentially a combination of existing technologies that are succeeding in make a paradigm shift in building and maintaining distributed computing systems making use of, multiprocessor, virtualization technology, network based distributed data storage and networking. The cloud providers have Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and many more services to offer[2] .

B. Cloud Security Issues

Cloud computing provides organizations with an efficient, flexible and cost effective alternative to hosting their own computing resources . However, hackers, attackers and security researchers have shown that this model can be compromised and is not 100% secure]. In a cloud, security is shared between the cloud provider and the cloud user. There are many security threats

which emerge inside or outside ofcloud provider's/consumer's environment and these can be broadly classified as Insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, and service disruption.

C 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 access control,symmetric cryprographic algorithm like DES,TDES,AES 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.

2.LITERAURE REVIEW

A number of studies showing the need of security in the Multimedia file storage in cloud computing.

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.

Wenchao et al. [3] in this paper have taken alternative perspective and proposed data centric view of cloud security. They have explored the security properties of secure data sharing among the applications hosted on clouds..

Wenwu Zhu et.al [4] 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 [6] 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.

Wayne [7]: In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services.

Chun-Ting Huang [9] 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.

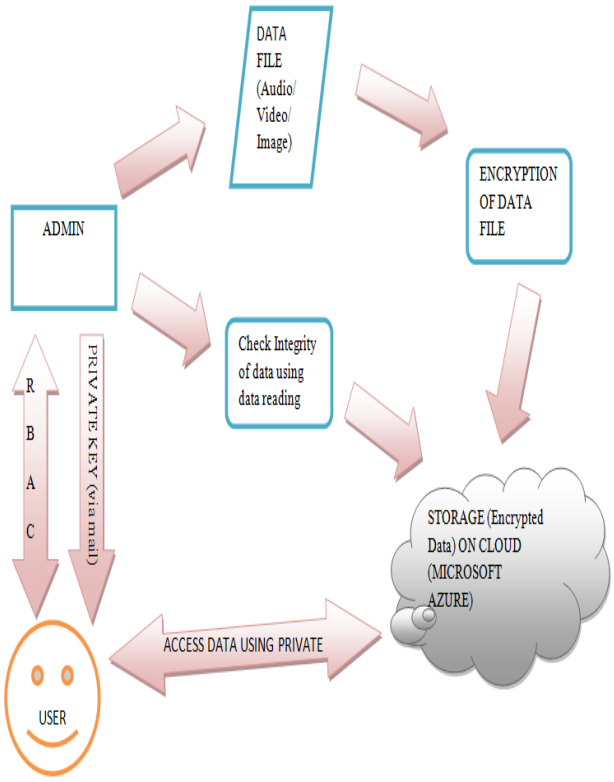
Neha Jain [10] presented a data security system in cloud computing using DES algorithm.

N. Saravanan et.al[11] presented a data security system in cloud computing using RSA algorithm. They have implemented RSA algorithm in google App engine using cloud SQL.

M. Sudha, Dr.Bandaru Rama Krishna Rao [12] implement a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality.

3.PROPOSED SCHEME

In this paper we proposed a secure cloud framework.. In our proposed approach we consider the security in the cloud side and also the client data is safe. For this we proposed an architecture . By using this architecture we can provide security to the cloud environment and to the user.



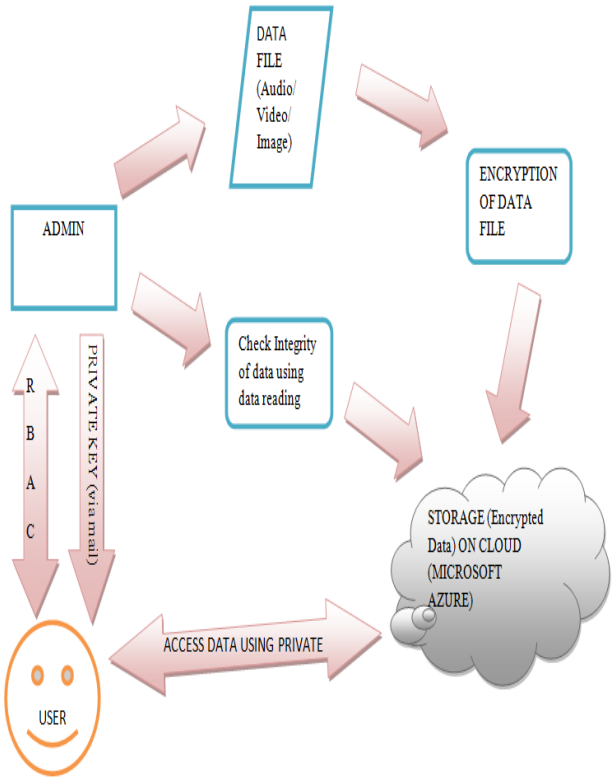


Fig 1:Proposed Scheme

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: -

- Design an encryption algorithm based on combination of RSA and AES (to have better security than RSA or AES alone) to encrypt the data files before storage on cloud (confidentiality)

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. User will be required to enter that private key which will be validated for that session only.This will provide enhanced security.

Reasons to choose RSA AND AES 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 AES algorithm over that so that the encryption standard may become quite sophisticated to get decrypted in a simpler manner.

Why AES?

AES is the most secured algorithm and also take the least time to encrypt data than others.

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.

4. HOW TO STORE DATA ON CLOUD?

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 and run the code.Set login page as start page as only authenticated users are allowed to store data on cloud.

5.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 architecture in which original file(text,audio,video) 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.

In this paper we taken two most secure algorithms RSA and AES 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) have been successfully uploaded and 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.

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] 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 .

[2] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA

[3] Sara Qaisar**;** "Cloud Computing :Network/Security Threats and Counter Measures, *Interdisciplinary Journal of Contemporary Research In Business, Jan 2012,Vol 3, No 9.*

[4] 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.

[5] 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.

[6] Tamleek Ali , Mohammad Nauman , Fazl-e-Hadi ,and Fahad bin Muhaya; "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm".

[7] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing , 44th Hawaii International Conference on System Sciesnces 2011.

[8] Zhang Mian, Zhang Nong; "The Study of Multimedia Data Model Technology Based on Cloud Computing"; 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

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