ISSN: 2319-7080 International Journal of Computer Science and Communication Engineering
Volume 2 Issue 3 (August 2013 Issue)

# Enhanced Multimedia Storage Scheme using RSA & PGP Algorithms for Cloud Computing

SatvirKaur, NitikaKapoor, Harish Kundra
[1]M.Tech Scholar, [2]Assistant Professor, [3]Associate Professor
[1, 2, 3] Rayat Institute of Engineering & Information Technology, Railmajra (Punjab), India
[1]satvir_rayat@yahoo.co.in, [2]er.nitikakapoor@gmail.com, [3]hodcseit@rayatbahra.com

***Abstract*: Number of users used Cloud to store their data. Data storage security is defining as the security of data on the storage media. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the malicious users so authentication of client becomes a mandatory task. In this paper, we proposed a new security scheme by using RSA & PGP algorithm. In this work, both these techniques help to generate a secure session key which is valid only for a single session. One more feature of security is added and that is Signature. In this when user stores their data they have to enter a unique signature which will make our scheme more secure and hence the new security scheme helps to increase the security at cloud.**

***Keywords* - Cloud Computing, Multimedia Storage Security, RSA, PGP, Signature.**

## I. INTRODUCTION

Cloud computing is an emerging technology aimed at providing various computing and storage services over the Internet [1], [2]. It generally incorporates infrastructure, platform, and software as services. Cloud service providers rent data-centre hardware and software to deliver storage and computing services through the Internet. By using cloud computing, Internet users can receive services from a cloud as if they were employing a super computer. They can store their data in the cloud instead of on their own devices, making ubiquitous data access possible. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud, mitigating the users' burden of full software installation and continual upgrade on their local devices.

With the development of Web 2.0, Internet multimedia is emerging as a service. To provide rich media services, multimedia computing has emerged as a noteworthy technology to generate, edit, process, and search media contents, such as images, video, audio, graphics, and so on. For multimedia applications and services over the Internet and mobile wireless networks, there are strong demands for cloud computing because of the significant amount of computation required for serving millions of Internet or mobile users at the same time. In this new 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 multimedia software maintenance and upgrade as well as sparing the computation of user devices and saving the battery of mobile phones.

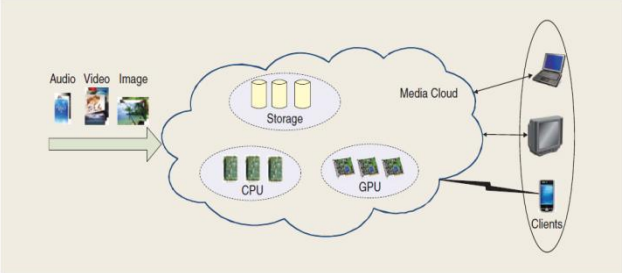


Fig 1 – Fundamental Concept of Multimedia Cloud Computing

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

- 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 transcoding and adaptation, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services for millions of users simultaneously.

- 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.

- 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.

- 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.

***Multimedia Aware Cloud***

The media cloud needs to have the following functions:
1) QoS provisioning and support for various types of multimedia services with different QoS requirements, 2) distributed parallel multimedia processing, and
3) Multimedia QoS adaptation to fit various types of devices and network bandwidth. In this section, we first present the architecture of the media cloud. Then we discuss the distributed parallel multimedia processing in the media cloud and how the cloud can provide QoS support for multimedia applications and services.

## II. MULTIMEDIA STORAGE SECURITY IN CLOUD COMPUTING

Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties, too. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them.The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. The safety of the files depends upon the hosting websites.

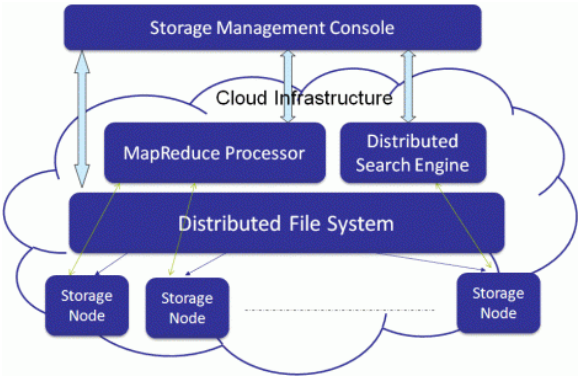


Fig 2: Cloud Storage Architecture

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface.

Cloud storage is:

- made up of many distributed resources, but still acts as one
- highly fault tolerant through redundancy and distribution of data
- highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas.

Data storage security refers to the security of data on the storage media, which means non-volatile or fast recovery after loss. This security should be taken into account by software engineers in design stage of cloud storage services. It includes not only data redundancy and dynamic, but also isolation. Redundancy is the most basic measures to protect data storage security, and dynamic means user data may often change, so effective measures are needed to ensure data consistency. Isolation is that since different user's data is stored in the same platform, to guarantee the independence between the data, which means user can only access their own data, and data changes of other users will not affect the current user.

***Major Risks of Cloud Computing Security***

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments.

Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic inspecific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

## III. PROPOSED SCHEME TO ENHANCE SECURITY IN MULTIMEDIA STORAGE

There are a number of security and Privacy issues/concerns associated with cloud computing but these issues fall into two broad categories: Security and Privacy issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security and privacy issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. It means that Security and Privacy are the major issues that are needed to be countered efforts are being made to develop many efficient System that can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. So, this work proposed enhanced approach using RSA & PGP algorithms. It also includes the signature to enhance the security.

### *3.1 Proposed Model*

The proposed modal focuses on following three objectives which are helpful in increasing the security on content/data storage and are simulated by visual studio environment using Cloud Environment.

- To develop a system those will Provide Security and Privacy to Cloud Data Storage.
- To Establish an Encryption Based System by using RSA & PGP for protecting Sensitive data on the cloud and Structure how data owner and storage Service Provider to operate on encrypted Data.
- To implement security by adding digital signature.
- To Develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption both the keys working at the user level.

In this proposed work, after login, the user can upload the text or image data only if the user is authenticated user. When user uploads any type of data then it is saved at window azure cloud in encrypted form using RSA & PGP algorithms.

### 4.2 Basic Workflow Design

Data Storage in Cloud Computing reached to very high level so; security is the need of the Cloud Environment. This proposed enhanced scheme use RSA& PGP algorithms and adds signatures to lock the data for more security.

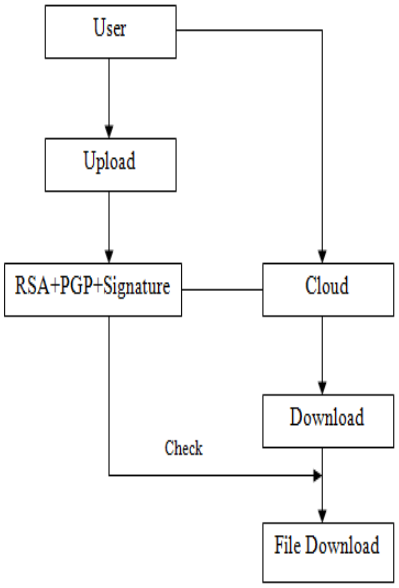


Fig 3: Basic Workflow Design of Proposed Work

This scheme is proposed to enhance the security in cloud data storage systems. The Block design of the proposed work is shown in Fig 3.

***User:*** A user can upload/ download file. When uploading file RSA & PGP Algorithms are used to increase security & digital signature is included to lock that data and when downloading file inverse RSA & PGP are used to decrypt data & digital signature is used to unlock the file.

### 3.3 System level Design

Fig 4 represents the system design of the proposed system with enhanced security scheme. In this figure uploading process of user is described.

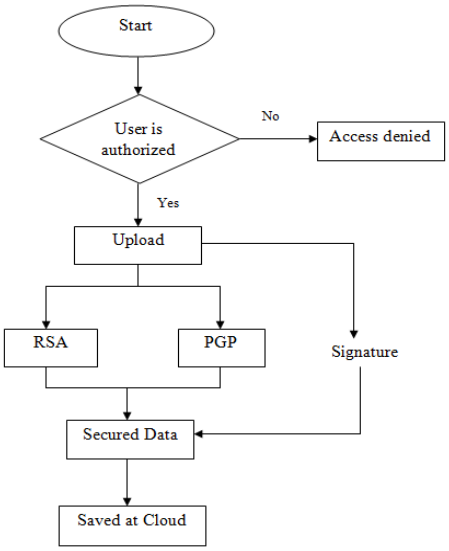


Fig 4: System level Design (user uploading) of proposed work

Figure 5 represents the system design of the proposed system with enhanced security scheme. In this figure downloading process of user is described.

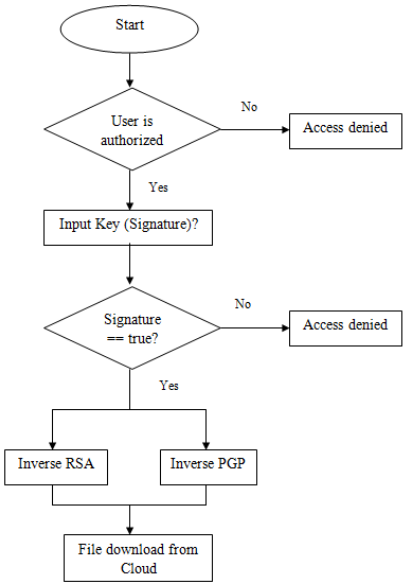


Fig 5: System level Design (user downloading) of proposed work

In this proposed system, user can download the file only if it is valid user with valid session. So because of this if in any case unauthorized person get access then he is not able to collect the data means data loss will be less.

## IV. RESULTS

This proposed model compare with the previous approach which uses a crossbreed algorithm and showing the results in Fig 6 and it concludes that this new enhanced approach using RSA & PGP Encoding schemes with digital signatures having better results. It means security level can be enhanced or improved with the help of this new scheme. This new enhanced scheme increase the security using RSA & PGP Encoding algorithms and with digital signature and results that it increases security & reduces data loss as well as unauthorized access.


Fig 6: Previous Approach & Enhanced Approach

## V. CONCLUSION

In this paper, we proposed a security approach, which is Enhanced Security Approach, for the cloud computing network to increase the security level & prevent from unauthorized access. Similarly, this enhanced approach can achieve better results than the previous approach which use crossbreed algorithm. It is expected that the data loss will be reduced using digital signature which is different for each file & enhanced security using RSA & PGP encoding schemes.

## VI. REFERENCES

[1] Academic Room.Cloud computing.www.academicroom.com/topics/cloud-computing.

[2] RSA Laboratories. Pkcs #5: Password-based cryptography standard.

[3]Qian Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li ,“Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[4] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in , cloud Computing”, 2010.

[5]M. Sudha, Dr. Bandaru Rama Krishna Rao, M.Monica, „A comprehensive approach to ensure secure data communication in cloud environment‟ International Journal of Computer Application (0975-8887), Volume 12- No 8, Dec 2010.

[6]PalivelaHemant , Nitin.P.Chawande, AvinashSonule, HemantWani,‟ Development of Server in cloud computing to solve issues related to security and backup‟, in IEEE CCIS 2011.

[7]Jianyong Chen, Yang Wang, and Xiaomin Wang, "On demand security Architecture for cloud computing", 0018-9162/12, published by the IEEE Computer society in 2012.

[8] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing" published by the IEEE computer and reliability societies in July/August 2009.

[9]NabenduChaki, "A Survey on Security issue in Cloud Computing " in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology, May 2009.

[10]Nils Gruschka and MeikoJensen ,"Attack surface : A taxonomy for attacks on cloud services" in 2010 IEEE 3rd international conference on cloud computing.

[11] Cong.Wang and KuiRenWenjing Lou and Jin Li "Towards Publicity Auditable Secure Cloud Data Storage".

[12]Dr.R.ManickaChezian and C.bagyalakshmi "a survey on cloud data security Using encryption technique" in International journal of advanced research in computer engineering & technology , Volume 1, Issue 5, July 2012.

[13]VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, "Data Security in cloud computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume 2, Issue 3, July2012.

[14]ParsiKalpana, SudhaSingaraju, "Data security in cloud computing using RSA algorithm", International Journal of research in computer and communication technology, IJRCCT, ISSN 2278-58,Volume 1, Issue 4, September 2012.

[15]Salvatore J. Stolfo, Melek Ben Salem, Angelos D. Keromytis, "Fog computing: Mitigating Insider data theft attacks in the cloud".

[16]Jonathan Katz,"Efficient cryptographic protocol preventing man in the middle attacks", Doctoral Dissertation submitted at Columbia university, ISBN: 0-493-50927- 5,2002.

[17] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *Above the Clouds : A Berkeley View of Cloud Computing*, 2009.

[18] J. Shneidman, C. Ng, D.C. Parkes, A. AuYoung, A.C. Snoeren, A. Vahdat, and B. Chun, "Why Markets Could (But Dont Currently) Solve Resource Allocation Problems in Systems," *Challenges*, 2005, p. 7.

[19] A. Das and D. Grosu, "Combinatorial auction-based protocols for resource allocation in grids," *Parallel and Distributed Processing Symposium, 2005.Proceedings.19th IEEE International*, 2005.

[20] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "*Ensuring Data Storage Security in Cloud Computing",* In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

[21] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, *"Cloud security issues*" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[22]Meiko Jensen, JlorgSchwenk, Nils Gruschkaand Luigi Lo Iacono, *"On Technical Security Issues In Cloud Computing",*IEEE International Conference on Cloud Computing,2009.

[23] J. Brodkin. Gartner: *"Seven cloud-computing security risks",*Infoworld, 2008.

[24] Vamsee Krishna and SriramRamanujam,*"Data Security in Cloud Computing",* Journal of Computer and Mathematical Sciences,vol. 2, Issue 1, 28 February, 2011.

[25] Hassan Takabi, James B. D. Joshi and Gail-JoonAhn**,** *"Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments"* Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, p.393-398, July 19-23, 2010.

[26] Jintao Liu,School of Electronics and Computer Science University of Southampton, *"Cloud Computing Security"* ,2009.

[27]Er. RimmyChuchra,Lovely Professional University,Phagwara, India, *"Data Security in Cloud Computing"*, International Journal Nov.,2012.

[28]Uma Somani, KanikaLakhani, Manish Mundra,*"Implementing Digital Signature with RSA EncryptionAlgorithm to Enhance the Data Security of Cloud in Cloud Computing"*, in 2010.