INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Security Scheme For Cloud Data Storage

Harjinder Kaur
Research Fellow, Sri Guru Granth Sahib World University,Fatehgarh Sahib, Punjab, India

Sarpreet Singh
Asst. Professor, Sri Guru Granth Sahib World University,Fatehgarh Sahib, Punjab, India

Abstract:

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. The multimedia storage system in a cloud centre is a cooperation storage service that contains multiple devices and application domains to reduce the operational cost and boost overall system performance.Security in data storage is one of the most important metrics in performance comparison of these cloud computing systems.To ensure the security of data, we proposed a method by implementing ACO which would be a combination of RSA & DES algorithm.

Key words*: Cloud Computing, Multimedia Cloud Computing, Data Security, RSA algorithm, DES algorithm, ACO.*

1.Introduction

The rapid development of the Internet has resulted in constant changes in wireless communication technology. With the rapid development of modern information technology to study how science to organize and store data, how to efficiently retrieve the data and database technology for data processing rapid changes have taken place.

1.1.Cloud Computing

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-center 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.

According to the National Institute of Standards and Technology (NIST) [3], cloud computing exhibits several characteristics:

- On-demand self-service- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- Rapid elasticity- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

As cloud computing is in its evolving stage, so there are many problems prevalent in cloud computing [4],[5]. Such as:

- Ensuring proper access control (authentication, authorization, and auditing)
- Network level migration, so that it requires minimum cost and time to move a job
- To provide proper security to the data in transit and to the data at rest.
- Data availability issues in cloud
- Legal quagmire and transitive trust issues
- Data lineage, data provenance and inadvertent disclosure of sensitive information is possible

1.2.Multimedia Cloud Computing

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.

Multimedia processing in a cloud imposes great challenges [6]. 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.

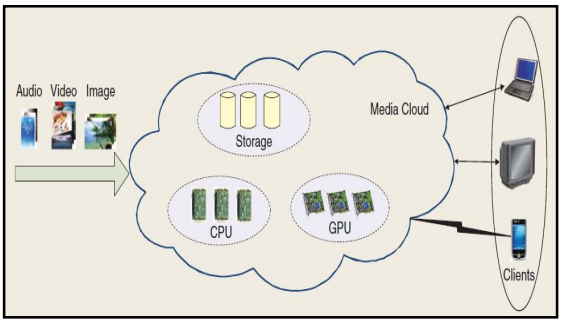

Figure 1: Fundamental Concept of Multimedia Cloud Computing

Multimedia cloud computing is generally related to multimedia computing over grids, content delivery network (CDN), server-based computing, and P2P multimedia computing. More specifically, multimedia computing over grids addresses infrastructure computing for multimedia from a high-performance computing (HPC) aspect [7]. The

CDN addresses how to deliver multimedia at the edge so as to reduce the delivery latency or maximize the bandwidth for the clients to access the data. Examples include Akamai Technologies, Amazon CloudFront, and Limelight Networks. YouTube uses Akamai's CDN to deliver videos. Server-based multimedia computing addresses desktop computing, in which all multimedia computing is done in a set of servers, and the client interacts only with the servers [8]. Examples include Microsoft Remote Display Protocol and AT&T Virtual Network Computing. P2P multimedia computing refers to a distributed application architecture that partitions multimedia-computing tasks or workloads between peers. Examples include Skype, PPlive, and Coolstream. The media cloud presented in this article addresses how the cloud can provide QoS provisioning for multimedia computing in a cloud environment.

2.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.

2.1.Multimedia Storage System

The multimedia storage system in a cloud computing center is a cooperation storage service that contains multiple devices and application domains to reduce the operational cost at the client-end and boost overall system efficiency. The basic architecture of a cloud storage system is composed by a storage resource pool, including the distributed file system, the Service Level Agreements (SLA), and service interfaces [9]. Moreover, the architecture can be decomposed into five layers based on their logical function boundaries as shown in Fig. 2. This layered model shows the delivery flow of stored data in a cloud server.

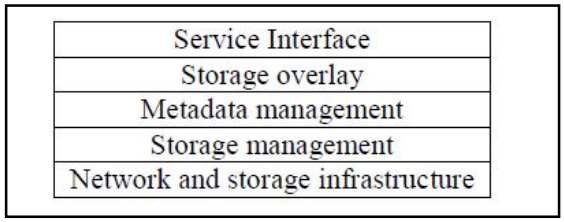

Figure 2: Cloud Storage layered model [9]

Many cloud computing and storage service providers are competing in the market, such as Amazon, IBM, Google, Sun Microsystems, Microsoft, EMC, HP, Symantec, etc. The cloud storage platforms developed by these companies are popular in the Internet such as SkyDrive, Amazon S3, HP Upline, Hitachi Content Platform, etc [10]. There are also many cloud storage platforms available in the market. A thorough performance comparison among these platforms is to be conducted. There are several performance metrics to be considered, including the cost-effectiveness in computing usage and storage usage. Clearly, security in data storage is one of the most important metrics in performance comparison of these cloud computing systems. If the provided cloud storage can be accessed or destroyed by malicious attackers, the service provider will lose trust from its users, and the leakage of personal data could cause great damage to each individual. Generally speaking, storage security consists of both physical storage security and data security. We will focus on data security issues in later sections since they can be attacked from the cyber space, which is of main concern in the modern information technology (IT) era.

3.Data Security Issues In The Cloud

3.1.Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

3.2.Data integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

3.3.Data Location And Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

3.4.Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

3.5.*Storage, Backup And Recovery*

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

The multimedia storage system in a cloud centre is a cooperation storage service that contains multiple devices and application domains to reduce the operational cost and boost overall system performance.Security in data storage is one of the most important metrics in performance comparison of these cloud computing systems.If the provided cloud storage can be accessed or destroyed by malicious attackers, the service provider will lose trust from its users, and the leakage of personal data could cause great damage to each individual.

Storage Security consists of:

- Physical Storage Security
- Data Security

4.Proposed Work

In Cloud computing, we have problem like security of data, files system, backups, network traffic, and host security. Here we are proposing a data security algorithm to implement ACO which would be a combination of

- RSA
- DES

which is going to increase the security.

In this proposed work,

- 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 and prevent replay attacks. (Run time authentication and prevention from replay attacks)

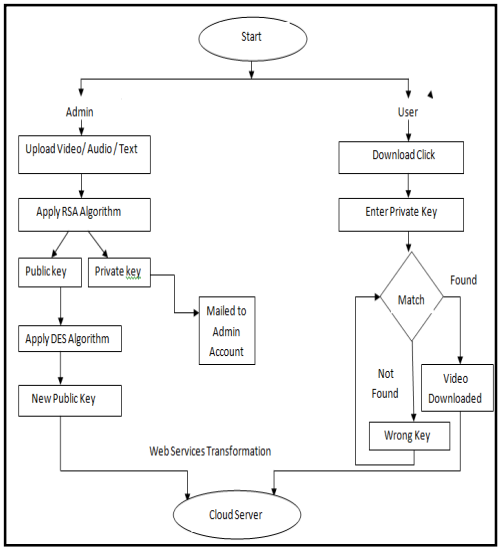

Figure 3: Algorithm level Design

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

The Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS) 46-3, Which Describes the data encryption algorithm (DEA). The DES has been extensively studied since its publication and is the most widely used symmetric algorithm in the world. The DES has a 64-bit block size key during execution. DES is a symmetric cryptosystem, specifically a 16-round Feistel Cipher. When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a Message Authentication Code (MAC). The DES can also be used for Single – user encryption, such as to store files on a hard disk in encrypted form .The DES has a 64-bit block size and uses a 56 bit key during execution.

5.Conclusion

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing ACO which would be a combination of RSA & DES algorithm.

6.Reference

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. 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 [Online] Available: http://radlab cs.berkeley.edu/
2. R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in Proc. 10th IEEE Int. Conf. High Performance Computing and Communications, 2008 pp. 5–13.
3. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.
4. T.R.V. Anandharajan, Dr. M.A. Bhagyaveni" Co-operative Scheduled Energy Aware Load-Balancing technique for an Efficient Computational Cloud" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.
5. Wayne Jansen Timothy Grance" Guidelines on Security and Privacy in Public Cloud Computing" NIST Draft Special Publication 800-144.
6. 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.
7. B. Aljaber, T. Jacobs, K. Nadiminti, and R. Buyya, "Multimedia on global grids: A case study in distributed ray tracing," Malays. J. Comput. Sci., vol. 20, no. 1, pp. 1–11, June 2007.
8. J. Nieh and S. J. Yang, "Measuring the multimedia performance of serverbased computing," in Proc. 10th Int. Workshop on Network and Operating System Support for Digital Audio and Video, 2000**,** pp. 55–64.
9. W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on cloud storage architecture and key technologies," in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009, pp. 1044-1048.
10. 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," Univ. of California, Berkeley, CA Technical Report No. UCB/EECS-2009-28, 2009.

11. Parsi Kalpana,Sudha Singaraju.,"Data Security in Cloud Computing using RSA Algorithm",International journal of Research in Computing and Communication technology,IJRCCT,ISSN 2278-5841,Vol 1,Issue 4,September 2012.
12. Neha Jain,Gurpreet Kaur"Implementing DES Algorithm in Cloud for Data Security".,International Journal of Computer Science&InformationTechnologyVSRD-IJCSIT,Vol.2(4),316-321,2012.
13. Esh Narayan,Mohit Malik,Aman Preet Singh"To Enhance the Data Security of Cloud in Cloud Computing using RSA algorithm" Bookman International Journal of Software Engg., Vol. 1 No. 1, ISSN No. 2319-4278, Sep. 2012.
14. Zhang Mian, Zhang Nong., "The Study of Multimedia Data Model Technology based on Cloud Computing" , 2nd International Conference on Signal Processing Systems (ICSPS), 2010.
15. Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo., "Multimedia Storage Security in Cloud Computing: an Overview" 978-1-457701434-4/11/$26.00,IEEE,2011.