Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing

Er. Mandeep Singh Sandhu
Asst. Prof. (Computer Engineering Section)
BMS College of Engg,Shri Muktsar Sahib, India

Er. Sunny Singla
M.tech CSE
BMS College of Engg, Shri Muktsar Sahib, India

Abstract— Most of our data is stored on local networks with servers that may be clustered and sharing storage. This approach has had time to be developed into stable architecture, and provide decent redundancy when deployed right. A newer emerging technology, cloud computing, has shown up demanding attention and quickly is changing the direction of the technology landscape. In our research work we have tried to work with the enhanced mode of security of the content which is going to be stored at cloud computing platform. The research has been done keeping the future aspects in mind. Today the cloud computing is a new arena and we all hoping it to be safe and secure. But we should not ignore the future aspects of the hacking systems and their methodologies. By keeping the future aspects in mind our work has distributed the data into different server platforms so that if someone tries to get to the data, he will have to access all the platforms provided for the data storage. A basic concept of advanced aco has also been introduced into our research work and we have applied the MD5 security algorithm along with the DES for the better encryption standard of our data. Characteristics of multimedia cloud computing and in the fifth section we analysis the RSA Algorithm & DES Algorithm. Finally we present the Conclusion & future works with the references.

Keywords— Cloud Computing; MD5; DES; Cryptography; Encryption; Decryption.

I. INTRODUCTION

Cloud computing multimedia database based on the current of database development, object-oriented technology and object-oriented fields in the database, increasing display its vitality[1].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. To comprehend cloud computing, an analogy to an electricity computing grid is to be useful. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable Computing resources. More exactly Cloud computing can be expressed as a combination of

Software-as-a-Service which perspective refers to a service delivery model in which remote component is used business services are accessible through a software interface and can be combined to create new business services delivered via flexible networks and Platform as a Service in which Cloud systems can offer an additional abstraction level: instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on and Infrastructure as a Service which Providers manage a large set of computing resources, such as storing and processing capacity. Through Virtualization, they are able to split, assign and dynamically re-size these resources to build ad-hoc systems as demanded by customers [2]. They deploy the software stacks that run their services.

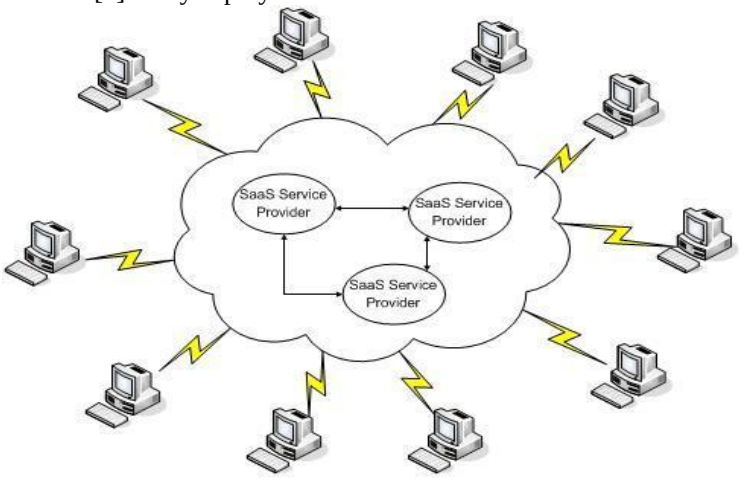

Figure 1: Cloud computing Technology

Cloud computing is an emerging technology aimed at providing various computing and storage services over the Internet [3]. 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 [4]. 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.

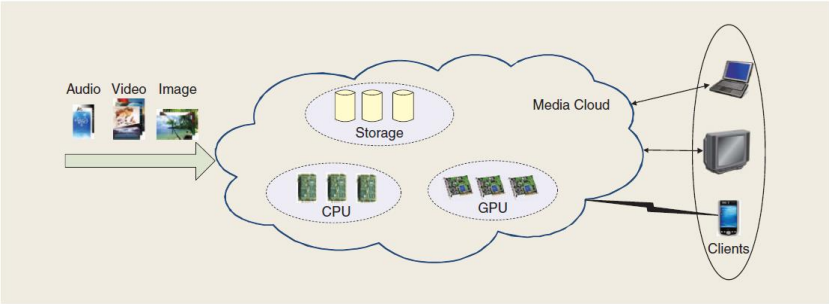

Figure: 2 – Fundamental Concept of Multimedia Cloud Computing

Multimedia processing in a cloud imposes great challenges. Several fundamental challenges for multimedia computing in the cloud are highlighted [5] 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 transcoding 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.

II. RELATED WORK

Multimedia file storage in cloud computing required the security. Multimedia cloud computing is termed as multimedia computing over grids, content delivery network (it is used for reduce the latency and increase the bandwidth of data), server-based computing, and P2P multimedia computing. It gives infrastructure of high-performance computing (HPC) aspect [6]. Desktop computing is Server-based multimedia computing addresses in which all multimedia computing is done in a set of servers, and the client interacts only with the servers [7]. Wenwu Zhu [8] is described the overview of multimedia cloud computing and it gives addressed multimedia cloud computing from multimedia-aware cloud. Multimedia-aware cloud presented how a cloud can provide QoS support, distributed parallel processing, storage, and load balancing for various multimedia applications and services. It proposed an MEC-computing architecture that can achieve high cloud QoS support for various multimedia services. On cloud aware multimedia, we addressed how multimedia services and applications, such as storage and sharing, authoring and mashup, adaptation and delivery, and rendering and retrieval, can optimally utilize cloud-computing resources. Jiann-Liang Chen [9] it proposed a novel IP Multimedia Subsystem (IMS) framework with cloud computing architecture for use in high quality multimedia applications. The IMS supports heterogeneous networking with Quality-of-Service (QoS) policy. 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. Hang Yuan [11] provides a comprehensive overview of the techniques and approaches in the fields of energy efficiency for data centers and large-scale multimedia services. The paper also highlights important challenges in designing and maintaining green data centers and identifies some of the opportunities

in offering green streaming service in cloud computing frameworks. Zhang Mian [12] presented the study that describes the cloud computing-based multimedia database and the different traditional database, object-oriented database model of the concept, discusses the cloud-based object-oriented multimedia database of two ways, and summarized the characteristics of such multimedia database model, superiority and development. Chun-Ting Huang [13] conduct a depth survey on recent multimedia storage security research activities in association with cloud computing. Neha Jain [14] presented a data security system in cloud computing using DES algorithm. This Cipher Block Chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. Results in order to be secure the system the communication between modules is encrypted using symmetric key.

III. PROPOSED WORK

In our proposed work , we are using a distributed framework architecture to make our data secure on the cloud platform . The mail service using the SMTP services has been used to make the data content secure from the unauthorized access.To save the original data , tow algorithm has been combined namely MD5 and DES.MD5 is one of the advanced security encryption schemes whose out is provided to the DES algorithm to make the data more encrypted so that the hacker is compelled to spend more and more time to access the data reference. On the other hand the original data has been put on the hosing service of the web application with a randomly generated lock whose key is dynamically send to the user's authorized mail . 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.

IV. CHARACTERISTICS OF MULTIMEDIA CLOUD COMPUTING [16]

4.1 Large-scalability

The scale of cloud is very large. The cloud of Google has owned more than one million servers and service is given to infinite users. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers and they provide much good services.

4.2 Virtualization of cloud computing

Cloud computing makes user to get service anywhere and anytime, through any kind of interface. You can complete all you want through net service using a computer or a mobile phone. Users can a use or share it safely through an easy way, anytime, anywhere. Users can complete a task quickly that can't be completed in a single computer.

4.3 Good reliability

Cloud uses data with multiplicity, it has good fault tolerant, and the computation of cloud has very ability so it has high reliability of the service. The use of cloud computing is more reliable than local computer.

4.4 Versatility

Cloud computing can produce different applications Running it at the same time with accuracy and good Productivity.

4.5 Extendibility

The scale of cloud can extend dynamically to meet the users. Increasingly, requirement and suggestions.

4.6. Service on demand:

Cloud is a big resource pool that you can buy according to your requirement and specification. Cloud is just like running water, gas, and electric that can be charged by the amount which you used.

V. MD5 ALGORIHM & DES ALGORITHM

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. According to the standard, it is "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later formulas, which are optimized for 32-bit machines. Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption .Figure 2 depicts this idea. It is necessary for security purposes that the secret key never be revealed.

To accomplish encryption, most secret key algorithms use two main techniques known as **substitution** and **permutation**. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called **rounds**. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of **S-boxes** which are basically non-linear

substitution tables where either the output is smaller than the input or vice versa. The DES algorithm is a basic building block for providing data security [20].

VI. Methodology

Features are the characteristics of the object of interest. Feature extraction methodologies analyze objects and images to extract the most prominent features which are representatives of the various classes of images. Following methodology is used to extract the features of the texture images.

STEP-1 First, pick the content and upload the content at cloud computing work.

STEP-2 To encrypt content using MD5 and further more the result is supplied to the DES algorithm

STEP-3 Send file reference to windows azure and key to unlock it to the mail service of the user using the SMTP protocol.

STEP-4 Combine all references to get the content

VII. Result

This paper proposes a more effective and flexible distributed verification scheme to address the data storage security issue in cloud computing. As it rely on the cryptography algorithms [MD5] and [DES] to be used. These algorithms are used for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission. This method achieves the availability, reliability and integrity of erasure coded data and simultaneously identifies misbehaving servers. There is a strong industry consensus that security, along with regulatory compliance is the barrier to the adoption of cloud computing. The needed breakthrough should mean customer's data is always encrypted, and the master encryption keys are themselves encrypted, even when in use .The combination on MD5 and DES of randomly generated secret Key encryption and homomorphism technologies are the secret sauce. To encrypt large messages a hybrid approach is used in which the messages are actually encrypted using symmetric schemes (MD5, DES etc.) and the key is transported using asymmetric schemes (MD5). In the algorithm that has been proposed here the effort has been in the direction of faster public key encryption without compromising the security of the system.

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[Online]. Available: http://radlab.cs.berkeley.edu/

[2] Vikas Goyal, Dr. Chander Kant, International Journal ofEngineering Sciences, ISSN : 2229-6913, September 2011,4, pp. 274-282. "Security Issues for Cloud Computing",

[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[Online]. Available: http://radlab.cs.berkeley.edu/

[4] 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.

[5] Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering (IJCSE), pp:1227 – 1231, Vol. 3 No. 3 Mar 2011, ISSN : 0975-3397

[6] 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.

[7] J. Nieh and S. J. Yang, "Measuring the multimedia performance of server based computing," in *Proc. 10th Int. Workshop on Network and Operating System Support for Digital Audio and Video*, 2000**,** pp. 55–64.

[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] Li Li, Xiong Li, Sun Youxia, and Liu Wen; "Research On Mobile Multimedia Broadcasting Service Integration Based On Cloud Computing".

[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] Hang Yuan, C.-C. Jay Kuo and Ishfaq Ahmad; "Energy Efficiency in Data Centers and Cloud-Based Multimedia Services: An Overview and Future Directions" 978-1-4244-7614-5/10/$26.00 ©2010 IEEE.

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

[13] 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.

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

[15] Information Engineering, Zhejiang Gongshang University, "A Hybrid Encryption Algorithm Based on DES and RSA" in Bluetooth Communication Second International Conference on Modeling, Simulation and Visualization Methods, 2010

[16] http://www.amazon.com/Enterprise-Cloud-Computing-characteristics/

[17] R.L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public- key Cryptosystems", Communications of the ACM, 21(2), 120-126, February 1978.
[18] RSA Laboratories, High Speed RSA Implementation, RSA Data Security, November 1994.
[19] Douglas R. Stinson, "Cryptography Theory and Practice", Chapman & Hall/CRC Press, 3rd Edition, pp. 211-214,2006.
[20] Eli Biham and Adli Shamir, "Differential Cryptanalysis of full DES".

