International Journal of Engineering Research & Technology (IJERT)
NCAEM-2013 Conference Proceedings
ISBN: 978-93-83758-09-8

Multimedia Security in Cloud Computing Environment Using RSA and DES Algorithm

[1]Anshul Arora, [2] Kamya Guglani
[1,2] M.tech Scholar, Geeta Engineering College Panipat

Abstract: Cloud computing is that emerging technology which is used for providing various Computation and storage services over the internet. The main advantages of clod computing is its performance, high availability and least costs, the data in Cloud Computing is stored in service providers so that the data can be easily accessed. But still many companies are not willing to use this technology because of the lack in security. This paper is written with the focus of improving the cloud computing security by two algorithms RSA (algorithm for public key cryptography) and DES (Data Encryption Standards, which is Private Key cryptography). This Paper is divided into Five main parts, the first part covers the Introduction of cloud computing and Fundamental concept of multimedia cloud computing. Second part covers the analysis about the related work already done; third part covers the proposed work which is to be done. Fourth part is the analysis of RSA and DES algorithm. The last part covers the Result along with the References.

Keywords: Cloud Computing, RSA, DES, cryptography, encryption, decryption, Multimedia Cloud Computing Environment.

I. INTRODUCTION

Cloud computing multimedia database is based on the current of database development, object-oriented technology and object-oriented fields in the database, which increasing display its vitality. Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing. To enabling convenient and on-demand network access to a shared pool of configurable computing resources are used for as a model of cloud computing. Cloud computing can be expressed as a combination of **Software-as-a-Service** which refers to a service delivery model to enabling used for business services of software interface and can be combined creating new business services delivered via flexible networks **and Platform as a Service** in which Cloud systems offering an additional abstraction level which supplying a virtualized infrastructure that can provide the software platform where systems should be run on and **Infrastructure as a Service** which Providers manage a large set of computing resources which is used for 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.

Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet. It generally incorporates infrastructure, platform, and software as services.

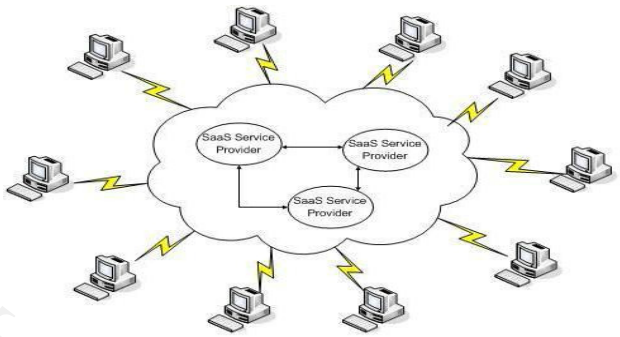

Fig. 1 Cloud Computing Environment

These service providers rent data-centre hardware and software to deliver storage and computing services through the Internet. Internet users can receive services from a cloud as if they were employing a super computer which be using cloud computing. To storing data in the cloud instead of on their own devices and it making ubiquitous data access possible. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud which mitigating the users' burden of full software installation and continual upgrade on their local devices. Internet multimedia is emerging as a service with the development of Web 2.0. 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 which provide rich media services. 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 new cloud-based multimedia-computing paradigm the 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. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows:

ISBN: 978-93-83758-09-8

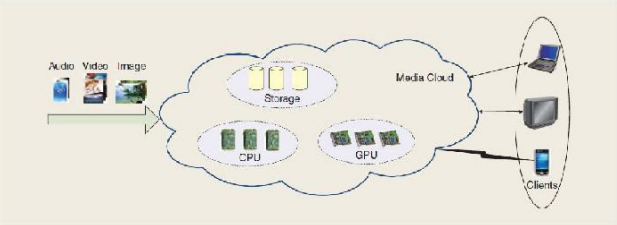

Fig. 2 Fundamental Concept of Multimedia Cloud Computing

1. Multimedia and service heterogeneity**:** The 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.

2. QoS heterogeneity**:** For different multimedia services different QoS requirements should be include and the cloud shall provide QoS provisioning which support for various types of multimedia services to meet different multimedia QoS requirements.

3. Network heterogeneity**:** The cloud shall adapt multimedia contents for optimal delivery to various types of devices with different network bandwidths and latencies which providing 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.
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 ALREADY DONE

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.
There are several important mechanisms meant to tackle with the various varieties of attacks. Even all those mechanisms as well as helpful for cloud computing. The cloud computing state of affairs is principally like client-server design. John Harauz, Lori M. George Simon Kaufman and Bruce Potter describe 3 basic mechanisms to safeguard the information security as follows:

- A tested Encryption/Decryption.
- Strict Access Mechanism
- A scheduled information backup theme.

A. On Demand Security Architecture
Jianyong bird genus, principle Wang Associate in Nursingd Xiaomin Wang demonstrated an efficient manner of providing information security to the user info keep at the cloud server by developing an new manner of On-demand security architecture. It defines security to be earned at 3 domains in cloud computing. Those 3 domains are mainly network, service and storage level. This storage unit is extremely versatile for the user. And additionally constant security is claimed to be user-transparent. Furthermore the user couldn't swear totally on the protection provided by the cloud services. Because how could the user know whether the data is being private by the service provider or not, if the personal info is attacked by some blackhat community for a few malicious act. So, several security measures may be taken during this regard. Although an efficient manner of providing security to the information store at cloud server however it's much terribly tedious task and it needs an excellent range of experience to develop different security levels that involve number of encryption/decryption algorithms. However once finished the above than it's very effective.

B. Hybrid Encryption Algorithms
Dr.R.Manicka Chezian and C.bagyalakshmi presents that just in case for a user to log into a system in cloud computing atmosphere as a login user one should give his/her login details at first by providing a username in plaintext kind. During this proposal, password is encrypted by the system as defined in algorithmic rule. In hybrid algorithm:

1. Password encryption by using Ceaser Cipher.
2. Repeat algorithm using RSA algorithmic rule.
3. Encrypt the resultant by mono alphabetic substitution methodology.

During this manner privacy to the secured cloud is provided and Developers will benefit by this method for better security. Though this method is better than other algorithms but if the size of text is increased its performance may sink.

C. Data Security using RSA algorithm.
Parsi Kalpana and Sudha Singaraju enforced RSA for securing the info in cloud computing. The most purpose of concern with this paper is a way to secure the information that is at rest in cloud computing. The complete method is categorized into three steps:

1. Key Generation
2. Encryption
3. Decryption

An effective cryptanalytic resolution for securing data. The key size isn't outlined within the work. If a bigger key size is provided then considerably the process speed of the algorithm get slower. Also, for larger key sizes it'll be troublesome to calculate the value of „e‟ . No easier resolution to seek out this value is mentioned.

D. Elliptic Curve Cryptography
Elliptic curve cryptography is mainly for the public key cryptosystem. Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi proposed a way by implementing digital signature and cryptography with elliptic curve cryptography. Thus

ISBN: 978-93-83758-09-8

authentication and encryption are the security solutions used in this system to secure information transmission from one cloud to another cloud. Elliptic curves indeed used enhancement to the diffie-hellman key exchange and digital signature algorithm.

E. Fog Computing for Data Security.

Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis proposed associate approach to secure the information using the Offensive Decoy Technology. This technique monitors completely different abnormal information access patterns and information access from cloud information storage. The most objective is to protect the user's real information against misuse. The methodology to secure cloud using decoy data technology is termed as Fog Computing. This technology is reused to detect misinformation attack that is used to stop the attacker knowing which one the real information and that one the phoney information. Here two completely different methods of fog computing to prevent sure attacks like the twitter attack are described. Initial one is that the cloud service supplier can deploy the decoy data among the cloud. And also the other is by deploying decoy data among personal on-line social networking profiles by the user. Whenever associate abnormal access to a cloud service happens, a cloud come back decoy data and delivers it as if it's fully legitimate and real. The decoy documents within the cloud server with the user's real information also will act as sensors to find out illegitimate access. This work applied the thought of illegitimate information access to data accessible on a local file system by some masquerades. Henceforth, the proposal makes use of user behaviour identification and decoy technology and also the analysis shows that combining each technique can yield higher detection result.

III. PROPOSED WORK

With this approach I am trying to secure the content which has been put over cloud. For this approach k/q ACO technique is being used. In this technique, the data content is being distributed on three servers and each server could only have the partial information about the other hardware.

We are using the hardware as follows:

- Web hosting server (could be go daddy as local host or any other).
- Gmail server for password security.
- Windows Azure.

As we will use different hardware for data security over cloud. For this work is being done in three modules.

MODULE 1:-

- To 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.

MODLE 2:-

- To design an encryption algorithm based on combination of RSA and DES encryption algorithm, to have better security then RSA and DES being used alone. This is being used to encrypt the data files before storage on cloud.

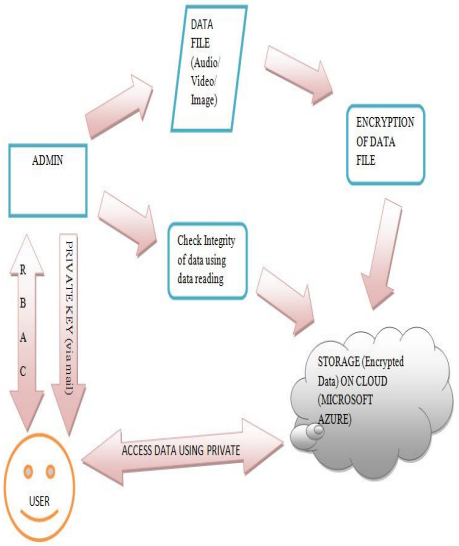

Fig. 3 How the Proposed Algorithm will work

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 and prevent replay attacks. (Run time authentication and prevention from replay attacks)
- Private Key in Module 1 is meant for authentication as well as it will prevent from Replay attacks as each time different private key will be generated for accessing the same data file.
- Hard Token may not suit the requirement because it can lead t leakage of token number. If , still you want, I can try that also.

IV. RSA & DES ALGORITHM

The RSA algorithm implements a public-key cryptosystem and digital signatures.RSA is a block cipher in which every message is mapped to an integer. RSA consists of public-key and private-key [17]. In Cloud environment the Public-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

1.) First, in Key generation before the data is encrypted, Key

generation should be done. This process is done between the Cloud service provider and the user.

2.) Second, in Encryption is the process of converting original plain text (data) into cipher text (data).

3.) Third, Decryption is the process of converting the cipher text (data) to the original plain text(data).

Why RSA?

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.

In the DES Algorithm there are two main types of cryptography.

1.) Symmetric key or secret key cryptography is the oldest type whereas asymmetric or public key cryptography is only being used publicly since the late 1970's.

2.) 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.

Why DES?

DES is an algorithm which generates sophisticated tree architecture to generate a encryption standard. It starts the encryption by taking the last node first node into the account, then the root node and finally the middle node, hence performing encryption node by node will lead to more security rather then including the Linear Array security.

What I tried to do:-

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

STEP-1 First, pick any text file, audio or video and upload these at cloud computing work.

STEP-2 To encrypt text file, audio or video, the cryptography RSA and DES algorithms is to be used.

STEP-3 Create architecture categories for system process.

STEP-4 Image, file or video is shown at Azure Cloud Computing.

V. CONCLUSION

This paper proposes a more flexible and effective algorithm for distributed verification scheme to address the data storage security in cloud computing environment. With this technique we can conclude that it can enhance the performance analysis of the multimedia content over the cloud. With the help of the encryption technique that is both RSA and DES algorithm the data on cloud computing environment will get more secure from the hackers. This method achieves the reliability, availability and integrity of erasure coded data and simultaneously identifies misbehaving servers. This technique will enhance the multilevel performance of the system architecture. It also provide better storage and searching technique for the multimedia contents over cloud architecture. In future , improvisation is possible over the submission of the private keys .In order to make it sure , work can be done to improvise the random generation of private keys so that at every access the private key is different and chances of getting hacked gets reduced. We have worked over the text, audio and video files. Furthermore an access control can be applied to this system so that the contents get saved from unauthorized access.

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] 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.

[8] Palivela Hemant , Nitin.P.Chawande, Avinash Sonule,Hemant Wani," Development of Server in cloud computing to solve issues related to security and backup" , in IEEE CCIS 2011.

[9] 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.

[10] 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.

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

[12] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi,"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.

[13] Parsi Kalpana, Sudha Singaraju, "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.

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

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

[16] 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.