International Journal of Pure and Applied Mathematics
Volume 119 No. 16 2018, 3257-3262
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Secured Data Transmissionin Cloud Using Hybrid Cryptography

Kranthi Kumar K[1], Devi T[2]
U.G Scholar, Assistant Professor
Department of Computer Science and Engineering
Saveetha School of Engineering, Saveetha University, Chennai.
Email_id: kranthikumarcube@gmail.com, devit.sse@saveetha.com

Abstract:

Now-a-days cloud computing is used to store large amount of data of many sectors like colleges, industries or military etc., in cloud users can able to retrieve any data, when user request for it. Cloud provides the users data whenever the user needed from anywhere over the internet. Due to huge advantages in the cloud many enterprises are using the cloud. Google, IBM, Oracle Corporation, Amazon Web Services, etc are the some of the Cloud Service Providers (CSP) which provides cloud services to the clients.Cloud resources are provided for the users based on their demand by the CSPs which are well known as third parties. Cloud consists of different deployment models like private, public, hybrid or community and different services such as IaaS, PaaS and SaaS.As the cloud technology is a third-party security stands as a major. Now the cloud technology was facing a problem of securing the stored data. Most of the cloud providers states that they are not amenable for security to the data, that means misplacing of the subscribed data or unjustifiedcorrections of data in the cloud. Researches are going on to provide better security to the client data in the cloud.

Keywords*: Cloud Computing, Hybrid Cloud.*

I. INTRODUCTION

Over past few years cloud technology is a internet based technology which evolved in the field of IT [1]. Cloud computing makes the exchange or capacity of vastdata simple to transfer and for usage.Cloudprovides adaptable "on demand service" to the clients over Internet. Cloud providesresources to the clients according to their request. Cloud enables clients to pay as per their necessity and need not pay for the not required resources. Organizations need not to pay exceptional equipment for sending diverse applications since cloud computing provides pay-as-you-go pricingbasis which implies that all of the resources like firewall, server, database etc. that are required by an organization for the sending of an application might be rented out by some other association which bargains in giving those resources.The latter organizations areknown as CSPs (Cloud Service Providers) [2]. Hence for leasing the cloud resources does not pay high cost andthe other organizations are also became very famous due to high end business on cloud. So, In IT sector cloud technology is the fast growing technology and it was attracting various organizations.

There are different deployment models and cloud services in which client can choose depending on their usage. These are discussed further.

1.1 Cloud Services

1.1.1 Infrastructure as a Service(IaaS):

IaaSprovidesmarketingapproch to vital web architecture, such as storage space, servers, and connections, without the business need of purchasing and managing this internet infrastructure themselves. Because of the economies of scale and specialization concerned, this could be to the advantage of all the business providing the infrastructure and also the one exploitation it [3]. especially, IaaS permits a web business the simplest way to develop and grow on demand.Both PaaS and SaaS mists are grounded in IaaS mists, as the organization giving the product as administration is likewise giving the foundation to run the product. Utilizing an IaaS cloud requests an eagerness to endure multifaceted nature, however with that intricacy comes adaptability. Amazon EC2 and Rackspace Cloud are cases of IaaS.

1.1.2 Platform as a Service (PaaS):

PaaS mists are made inside IaaS Clouds by authorities to render the adaptability and sending of any application minor and to help make your costs versatile and unsurprising. A few cases of a PaaS framework include: Mosso, Google App Engine, and Force.com.The main advantage of an administration like this is for as meager as no cash you can start your application with no pressure more than fundamental improvement and perhaps a

bit of porting in the event that you are managing a current application and PaaS permits a great deal of versatility by outline because of base on distributed computing [3]. The most vital negative of utilizing a PaaS Cloud supplier is that these administrations may actualize a few confinements or exchange offs that won't work with your item under any conditions.

1.1.3 Software as a Service (SaaS):

SaaS is moderately developed, and the expression's utilization originates before that of distributed computing. Cloud applications enable the cloud to be utilized for programming engineering, diminishing the weights of upkeep, support, and activities by having the application keep running on PCs having a place with the seller [3]. A portion of the cases for SaaS are Gmail and Salesforce, however not all SaaS must be situated in distributed computing.

1.2 Deployment Models

The deployment models in cloud computing are divided into four, which are:

1.2.1 Private Cloud: It is the one in cloud infrastructure is established among the organization and provides restricted access to the users. Since, authorised privileged users get access the resources on the cloud, it is considered as most secure of all other deployment models. It is deployed where the number of users accessing the information is small.

1.2.2 Public Cloud: It is the one in which cloud infrastructure is shared among different organizations. The public cloud is managed by some third party who lease out the resources to the organizations as per their demand. Hence, the public cloud supports the feature pay per usage. Public clouds are vulnerable to data tampering as there are multiple organizations accessing the applications on sharing basis and hence, it may give easy access to some intruder.

1.2.3 Hybrid Cloud: As the term Hybrid states that it consists of two or more cloud technologies.It offers the benefits of all the cloud models. It provides ability to maintain the cloud as recovery of data is easy in this cloud. It offers more flexibility than both public and private clouds. [4]

1.2.4 Community Cloud: The organizations and companies which are working on same interest or same working field will make use of community cloud environment. The organizations having samerequirements (like security, policy, etc.) agree to share the resources from the same party orCSP. So, community cloud is simply known as public cloud with additional security and quite similar to private cloud. The infrastructure may be maintained within the organizationor outside the organization [2].

II. LITERATURE SURVEY

A) Sunita Rani and AmbrishGangal,[5] "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints" proposed a hybrid algorithm for securing the user data initially the message will be encrypted with the ceaser cipher and the result will be encrypted with the RSA algorithm and result will be again encrypted with mono alphabetic substation method.

B) Vinita Keer, Dr. Syed Imran Ali, Prof. Neeraj Sharma [7], "Hybrid Approach of Cryptographic Algorithms in Cloud Computing", the main moto of their work is to secure the data files in the cloud while storing into the cloud.Ceaser ciphering technique is used for initial level security in this model, in the second level new designed encryption algorithm was used for encrypting the data and in the third level concentrates on authentication of the user. XOR operation, DES, RSA, IDEA algorithms are used for the encryption process.

C) Priyajaiswal, Randeepkaur, Ashok Verma,[8] "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique", in their proposed model classical encryption technique used in their algorithm. The main moto of their work is to increase the space complexity of the data in the cloud storage. This model follows the step by step process, initially finding the ASCII value, creating a square matrix, adding the key value to the divided matrices, performing the top, bottom and diagonal triangle operations and finally converting into ASCII code.

D) Dr. L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" [6], these models mainly improve the classical encryption techniques by using substitution cipher and transposition cipher. Initially the data will be converted into ASCII code and result will be divided into matrix format and performing the key transposition operations and finally will again converted into ASCII code, now the same process will be done for one more time for data encryption process.

E) Jasleen Kaur and Dr. Sushil Garg, "Security in Cloud Computing using Hybrid of Algorithms" [1], in the proposed work blending withDigital Signature with RSA algorithm and Blowfish

algorithm. Initially a hash is framed to create message digest, for sign the document RSA private key algorithm was used for encryption and for verifying the document Blowfishalgorithm was used.

III. PROPOSED WORK

To decrease the time complexity for data encryption and decryption in the cloud a new Hybrid cryptographic method was introduced. In this paper AES and DES algorithms are used for encryption, initially the input data (data which is to be encrypted) divided into two different parts and made it as separate files. Each file is encrypted with different algorithms i.e., first half or file is encrypted with DES algorithm and second half or file is encrypted using AES algorithm, then both the results are taken and two of them are combined together and encrypted by using key. Here the most important task is to secure the key, so for securing the key, image stenography LSB process is used. The key information is shared via email with the user as a image format. All these process will comes under the Encryption process.

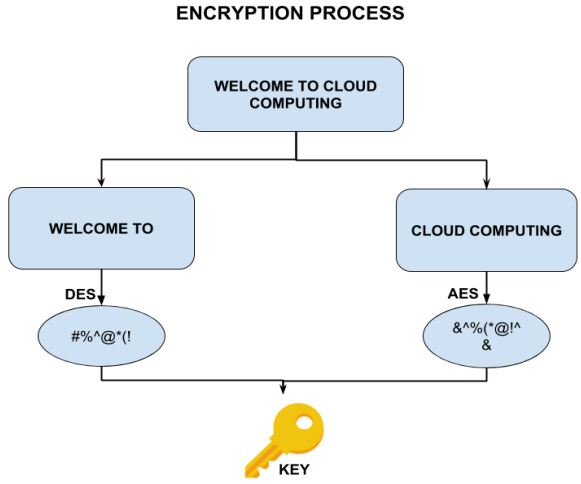

Fig: 3.2.1 Encryption Process with AES and DES algorithms

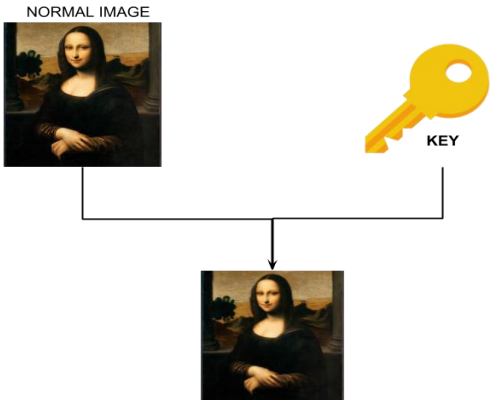

Fig: 3.2.2 Securing Key using image steganography technique

At the decryption side the user will receives the key information by mail. The key will be embedded in the image and the user will extract the key from the image using image steganography technique and by using the key the user will decrypt the DES and AES encrypted files and after that the data can be decrypted with their respective files algorithms i.e., DES, AES and finally the exact data of two different files can be combined together to read the data.

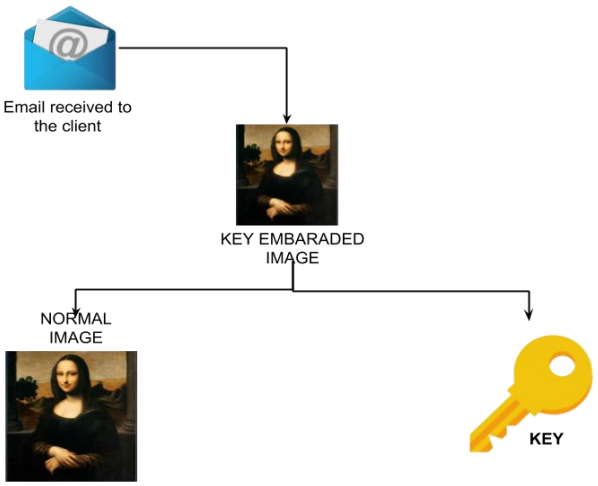

Fig: 3.2.3 User receives the key via email which is embedded in the image

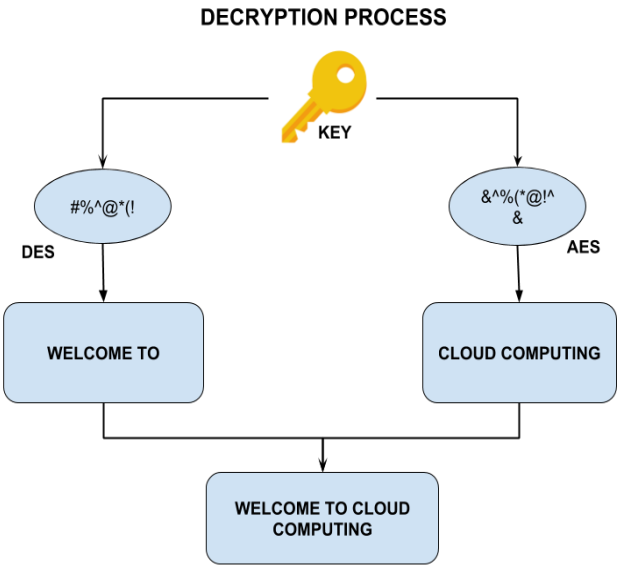

Fig: 3.2.4 Decryption process by using key and combining the complete message.

3.1 Architecture

The below architecture represents the overall working process of the encryption and decryption on both client and server side in the cloud to provide better security to the data while transmitting.

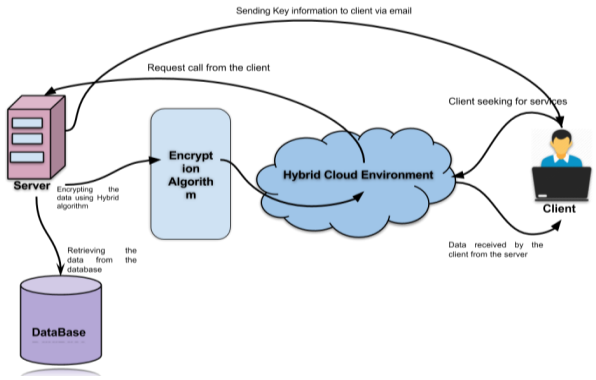

Fig: 3.3.1 Working of Encryption and Decryption Process in the cloud environment

IV. CONCLUSION

Cloud technology is the most rapid growing technology in the present generation. In day to day life cloud is the most important technology which helps our daily works easier and simple, by using cloud users can able to complete big task with a simple solution. As in the same way there are some of the draws for the cloud technology which made a situation to use the cloud or not. Security is the most important issue in the cloud technology, researches are going on for providing the better security to the cloud data and many new techniquesandalgorithms are introduced as seen from the previous works. So in future the cloud technology will increase by providing better security to the user data.

V. REFERENCES

[1] Jasleen Kaur and Dr. Sushil Garg, “Security in Cloud Computing using Hybrid of Algorithms” International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015.

[2] Jasleen Kaur and Dr. Sushil Garg, “Survey paper on security in Cloud computing”, International Journal In Applied Studies AndProduction ManagementVolume1, Issue 3, 15 May- 15 August 2015.

[3] http://www.monitis.com/blog/3-types-of-cloud-computing-services/

[4] Kaur, Jasleen, AnupmaSehrawat, and Ms Neha Bishnoi. "Survey Paper on Basics of Cloud Computing and Data Security." International Journal of Computer Science Trends and Technology (IJCSTT) (2014).

[5] Sunita Rani and AmbrishGangal, “Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012.

[6] Dr. L. Arockiam, S. Monikandan “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[7] Vinita Keer, Dr. Syed Imran Ali, Prof. Neeraj Sharma, “Hybrid Approach of Cryptographic Algorithms in Cloud Computing”,International Journal of Emerging Technology and Advanced Engineering.

[8] Priyajaiswal, Randeepkaur, Ashok Verma, “Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique”, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 1, January 2014)

[9] http://en.wikipedia.org/wiki/Category:Cloud_computing_providers
[10] Zunnurhain, Kazi, and Susan V. Vrbsky. "Security in cloud computing." Proceedings of the 2011 International Conference on Security & Management. 2011.
[11] Kaur, Jasleen, AnupmaSehrawat, and Ms Neha Bishnoi. "Survey Paper on Basics of Cloud Computing and Data Security." International Journal of Computer Science Trends and Technology (IJCSTT) (2014).
[12] http://cloudcomputingcafe.com/
[13] Zissis, Dimitrios, and DimitriosLekkas. "Addressing cloud computing security issues." FutureGeneration computer systems 28.3 (2012): 583-592.
[14] SO, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks (2011): 11-14.
[15] Khedia, Saurin, and Nishant Khatri. "A Review on Hybrid Techniques of Security In Cloud Computing."
[16]http://www.verio.com/resource-center/articles/cloud-computing-benefits/