ISSN:0975-9646

Enhanced Security for Multi Cloud Storage using AES Algorithm

Namita N. Pathak [1], Prof. Meghana Nagori [2]

[1]*PG Student (CSE),* [2]*Asst. Professor (CSE)*

[1, 2]*Department of Computer Science & Engineering Government College of Engineering Aurangabad, India.*

***Abstract*— The use of cloud computing has increased rapidly in most of the organizations. Security is considered to be the most important feature in a cloud computing environment because of the sensitive information stored in the cloud for users. The goal of cloud security is mainly to concentrate on the issues related to the data security and privacy features in cloud computing. The multi cloud model is based on data storage on distinct cloud by splitting files into different chunks then encrypts data using AES algorithm and MD5 technique is used for verification of data with two cloud servers. [1]**

***Keywords*— AES, MD5, private cloud, public cloud, and hybrid cloud.**

I. INTRODUCTION

Cloud computing is a model for enabling on-request access to a shared pool of configurable computing resources. Cloud computing and storage solutions give users and enterprises with various abilities to store and process their data in third-party data centers. It depends on sharing of resources to achieve consistency and economies of scale, similar to a utility over a network. The goal of cloud computing is to allow users to take advantage from all of these technologies, without the need for more knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users to concentrate on their core business instead of being impeded by IT obstacles.

Cloud computing can enable a user to access applications and data from any computer at any time since they are stored on a remote server. It also minimize the need for companies to acquire top-of-the-line servers and hardware or hire people to execute them since it is all maintained by a third party.[2]

Cloud computing is derived from earlier large-scale distributed computing technology. NIST defines Cloud computing as "a model for providing suitable, on request network access to the computing resources like networks, storage, applications and services that can be rapidly delivered and released with minimum management effort or service provider cooperation". In Cloud computing, files and software are not fully carried by the user's computer. File security concerns occur due to both user's application and program are laid in provider premises. The cloud supplier can solve this problem by encrypting the files by using encryption technique.

A. Types of Cloud Computing

1) Private Cloud

Private cloud is cloud structure operated only for a single organization, whether managed internally or by a third-party, and provided either internally or externally. Undertaking a private cloud project requires a outstanding level and degree of commitment to virtualized the business environment, and requires the company to re-evaluate decisions about existing resources. These resources have to be refreshed periodically, resulting in additional capital expenditures.

2) Pubic Cloud

A cloud is public when the services are provided over a network that is open for public use. Public cloud services may be free. Technically there may be small or no difference between public and private cloud architecture, however, security consideration may be significantly different for services that are made available by a service provider for a public viewers and when communication is achieved over a non-trusted network.

3) Hybrid Cloud

Hybrid cloud is a combination of two or more clouds like private, community or public that remain different entities but are kept together, giving the benefit of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, tried to keep or to dedicate services with cloud resources.

II. LITERATURE SURVEY

Cloud computing offers dynamically expandable resources delivered as a service over the Internet. The third party, on-request, self-service, pay-per-use, and logically scalable computing resources and services offered by the cloud paradigm promise to minimize capital as well as operational overheads for hardware and software.[3]

Cloud computing is the general term for anything that includes the provision of the hosted services over the internet. Cloud computing proposes a new and exciting way of computing with various service models that enables different services to the users. While all the data of an organization processed remotely and exchanges via different networks. Security is a critical parameter and the service provider must ensure that there is no unauthorized

user access to the important data of an organization during the data transmission. [9]

Cloud computing provides a replacement of computing with distinct services models that enables completely different services to the users. As all the information of associate degree organization processed remotely and transfer via completely different network. Security is important parameter and also the service provider makes sure that there no authorized access to the important information of associate degree organization throughout the information. Cloud computing is the approach of using remote servers on the internet to manage, store and process data instead of using a personal computer.

A. Analysis of Existing Systems

Reema Gupta and Tanisha contributed the concept of file security model which uses the concept of hybrid encryption scheme to meet security needs. In this model, encryption and decryption of files at cloud server is done using blowfish and modified version of RSA. Further, it is tested in cloud environment. [4]

Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen demonstrate Security and Privacy-Enhancing Multicloud Architectures. This system provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various different architectures are introduced and discussed according to their security and privacy capabilities and expectations. [5]

S. Subbiah S. Selva Muthukumaran and T. Ramkumar represented An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm. The vertical partitioning algorithm is used to protect the data in an efficient manner. The algorithm has been executed in a java platform and results are compared with the other algorithms. [6]

Miss. Priyanka.R.Raut, Prof. Vaidehi Baporikar aims to design and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System. In this system, they are executing the ideas of various cloud storage beside with enhanced security using encryption methods otherwise storing complete file on single cloud system. [7]

III. RESEARCH METHODOLOGY AND PROPOSED SYSTEM

The goal of cloud security is mainly to concentrate on the issues related to the data security and privacy features in cloud computing. In proposed system the multi cloud model is based on data storage on distinct cloud by splitting files into different chunks then encrypts data using AES algorithm and MD5 technique is used for verification of data with two cloud servers. [10]

A. *AES Algorithm*

AES (Advanced Encryption Standard) is a symmetric encryption technique. The algorithm was proposed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be effective in both hardware and software; AES is block cipher which supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES algorithm operates on a 4×4 column-major order matrix of bytes, called as the state.

Algorithm:

1. Key Expansion—round keys are obtained from the cipher key using Rijndael's key schedule. AES needs a separate 128-bit round key block for each round plus one more.

2. Initial Round and AddRoundKey—each byte of the state is merged with a block of the round key using bitwise xor.

3. Rounds Sub Bytes—the non-linear substitution step in which each byte is returned with another using a lookup table.
   Shift Rows—a transposition step in which the last three rows of the state are moved cyclically a definite number of steps.
   Mix Columns—a mixing operation which performs on the columns of the state, merging the four bytes in each column.
   AddRoundKey

4 .Final Round (no Mix Columns)
   Sub Bytes
   Then Shift Rows
   And AddRoundKey.[8]

B. *Structure of Proposed System*

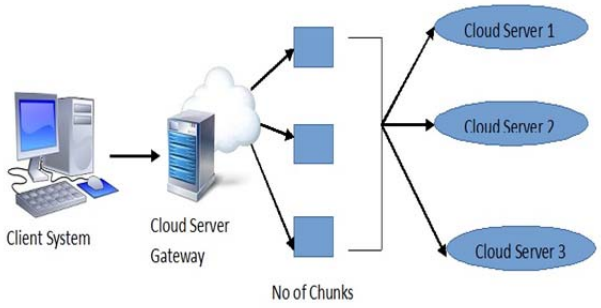

Fig 1 A general framework of proposed system

The architecture of proposed system involves three different modules like client module, cloud server gateway module and cloud storage module. In first module client will create the file which is to be stored on cloud server gateway. Cloud server will divide this file into number of chunks which is to be encrypted using AES symmetric key algorithm. Rather storing complete file on single cloud system will split the file in different chunks then encrypt it and store it on different cloud and the Meta data required for decrypting and rearranging a file will be stored in metadata management server.

IV. CONCLUSION

Many businesses related security and safe storage problems will be solved by implementing cloud based storage. But by expert advice it is more risky to put the data on single cloud as it increases the possibilities of different user attacks.

So by implementing the proposed system we are increasing the cloud storage security by sharing and encrypting the data. This system uses the concept of multiple cloud storage along with enhanced security using encryption algorithm where rather than storing complete file on single cloud system it will split the file in number of chunks then encrypt it and store on different cloud.

REFERENCES

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] Prof. J. M. Patil and Ms. B. S. Sonune "Data Security using Multi Cloud Architecture" International Journal on Recent and Innovation Trends in Computing and Communication may 2015.

[3] J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi-cloud Architectures" IEEE Transactions on Dependable and Secure Computing,Vol. 10, No. 4, July/August 2013.

[4] Reema Gupta, Tanisha and Priyanka "Enhanced Security for Cloud Storage using Hybrid Encryption" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.

[5] Elham Abd Al Latif Al Badawi & Ahmed Kayed "Survey on Enhancing the Data Security of the Cloud Computing Environment by Using Data Segregation Technique" IJRRAS May 2015.

[6] S. Subbiah S. Selva Muthukumaran and T. Ramkumar "An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm" Middle-East Journal of Scientific Research 23 (2): 223-230, 2015.

[7] Miss. Priyanka.R.Raut and Prof. Vaidehi Baporikar "Design and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

[8] Nisha D. Dable and Nitin Mishra "Design and Implement Enhancing Security in Multi Cloud Storage System using Distributed File System" International Journal of Computer ApplicationsVolume 103 – No 13, October 2014.

[9] Rajkumar B and Balamurugan K "Service and Data Security for Multi Cloud Environment" International Journal of Innovative Research in Computer and Communication Engineering March 2014.

[10] Sasikumar Gurumurthy, T. Niranjan Babu and G. Siva Shankar "An Approach for Security and Privacy Enhancing by Making Use of Distinct Clouds" International Journal of Soft Computing and Engineering (IJSCE) Volume-4, Issue-2, May 2014.