ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, May 2016

The security issues for cloud computing security single to multicloud by using AES Algorithm

***Prof.R.B.Rathod*, Vijaya Shendage, Swati Patil, Kirti Sakhare, Swati Kolhe.**

Abstract— Cloud computing is defined as a type of online computing that believes in sharing computing resources, processing power and storage based on demand rather than dependent on local servers to provide these facility, like as Making Cloud of Clouds is a recent concepts mixing combine services from multiple clouds into a single cloud. To avoid the problems of single Cloud Computing, such as no guaranty of continuous availability of data resources and services. Recently we are using MULTI-CLOUD facilities. Because it provides high rate of availability and good performance, but still this Multi-cloud environment have less Security issues. To avoid the problem of security issues some protection schemes should be adopted. This paper mainly focuses on many security issues of data storage in the "Cloud computing" and "Multi-Cloud computing" and also on AES security algorithms.

***Index Terms*. : Cloud Computing, Cloud Storage, Multi-Cloud Computing, Security, AES Algorithms.**

I. INTRODUCTION

" The Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provided and released with minimum management effort or service provider interaction". Cloud has some characteristics such as,

• On-demand self-service

• Broad network access

• Resource pooling

• Location independence

• Measured service

• Rapid elasticity

The Cloud Computing is classified into four category models like as Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Public Cloud can access everyone and Private cloud is restricted only a specific users. Hybrid models are combination of Public and Private Cloud models. Application for Community cloud by some community organization such as education, medical, etc.They shown in following fig:

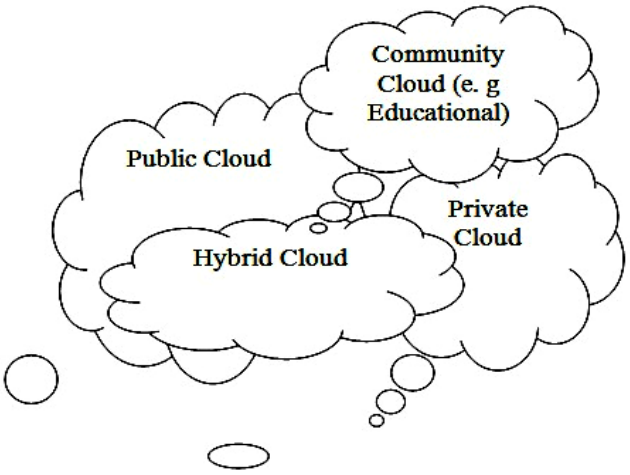

Fig a: cloud model

Cloud computing is a ubiquities architecture that can be centralizes server resources on a scalable platform so as to provide on demand computing resources and services. The cloud providers offer three types of services like as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Encryption techniques used previously are RSA based, which have different problems which can be overcome by using the most powerful encryption techniques. I.e it uses advanced encryption standards (AES) encryption Algorithm. AES is most frequently used encryption algorithm now day this algorithm is based on several Methods, linear transformations and permutations, each executed by data blocks of 16 byte. Therefore, AES remains the preferred encryption standard for governments and also banks and high security systems in the world.

.

II. PROBLEM STATEMENT

The concepts used for security purpose doesn't lead to provide more security. But the main issue of security is does not overcome so the concept of single cloud to multi-cloud is used to store the data and to prevents security.They providing security is main issue in cloud computing. In the previous more research has been conducted into single clouds than into multi clouds but in single cloud there is more possibility of security risks than in multicloud.To overcome the limitation concept of file splitting is used for security purpose. AES .Encryption algorithm is used to provide security to files.

III. SYSTEM ARCHITECTURE

Figure shows the system architecture of proposed System**.**

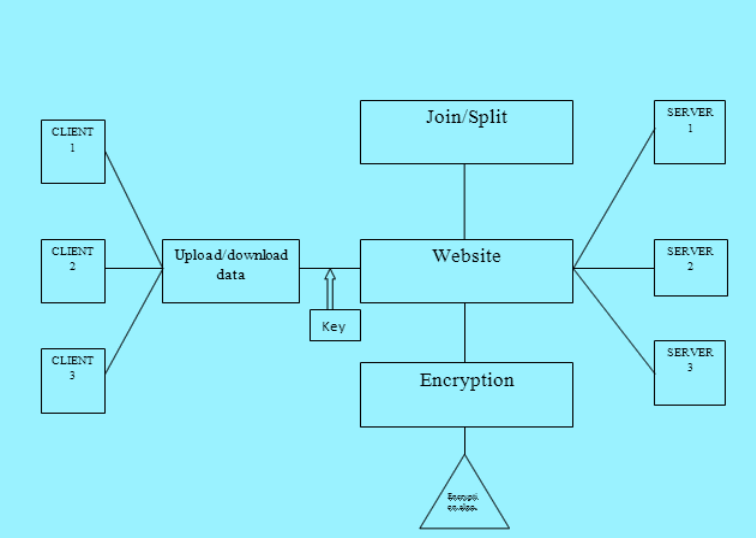

Fig b System Architecture

The proposed scheme works in following Steps:

1) The User should register on the website.

2) System will be sending a verification link on user email id.

3) After verification the user will be able to upload and download file.

4) Then the user tries to upload a file he has to input a key for encryption algorithm that time it will encrypt the data.

5) Ones the data is encrypted the system will distributed the file into multiple parts according to the number of IAAS servers and store in individually in different servers.

6) If the user wants to download a file he should place the password and the file will be called back on the client side and to download the files.

IV. AES ALGORITHM DESCRIPTION

AES on a style principle referred to as a linear transformation and permutation network, combination of each linear transformation and permutation, and it is quick in each package and hardware and also block size of 128 bits, and a key size of 128, 192, or 256 bits.

it will be any multiple of 32, each with bits a minimum of 128 and a higher of 256 bits.

AES operates on a 4×4 column-major order matrix.

ALGORITHM:

Steps:

- **Key Expansion:** the round keys are derived from the cipher key.it requires a separate 128-bit round key block for each round plus one more.
- Initial Round:
  Add Round Key each byte of the state is combined with a block of the round key using bitwise xor operator.
- **Sub Byte:** a non-linear transformation step where each byte is replaced with another according to a lookup table.
- **Shift Rows:** a transposition step where the last three rows of the state are shifted sequentially a certain number of steps.
- **Mix Columns:** a mixing operation which operates on the columns of the state then combining the four bytes in each column.
- and also Final Round

  Sub Bytes

  Shift Rows

  Add Round Key.

V. LITERATURE SURVEY

Paper	Existing System	Proposed System	Key mechanism and Methodology Used	Advantage	Limitations
"Collaboration in Multi-cloud Computing Environments: Framework and Security Issues", [2013]	Cloud includes applications delivered as Services	Cloud mash-ups is recent trend. It combines services from multiple clouds into a single service or applications. It used proxies	1. Establishing trust and secure delegation. 2. Policy heterogeneity and conflicts.	To facilitate dynamic collaboration between clouds	Refining of proxy deployment scenario and operation components

"Collaboration in Multi-cloud Computing Environments: Framework and Security Issues", [2013]	Cloud includes applications delivered as Services	Cloud mash-ups is recent trend. It combines services from multiple clouds into a single service or applications. It used proxies	1. Establishing trust and secure delegation. 2. Policy heterogeneity and conflicts.	To facilitate dynamic collaboration between clouds	Refining of proxy deployment scenario and operation components
"Hybrid Multi-cloud data security (HMCDS) model and data classification" ,[2013]	When the number of cloud users increases this may be lead to data security and privacy threats	When the number of cloud users increases this may be lead to data security and privacy threats	When the number of cloud users increases this may be lead to data security and privacy threats	Best part of its that it access only required data	This paper not testing data retrieval deficiency. Not providing best data classification technique.
"Security Issues and Security Algorithms in Cloud Computing",[2012]	Security Concerns:- Data, Access, Data Classification and Service Level Agreement	Cryptographic algorithm are used to hide the data and to restrict the data	RSA, DES, AES, BLOWFISH, 3DES and Shamir secret key algorithms.	Mentioned algorithms difficult crack without static passwords	Mentioned algorithms difficult crack without static passwords
"Using Secret Sharing Algorithm for Improving Security in Cloud Computing",[2014]	Multi-cloud architecture HAIL,RACS faces some problem	Dep-Sky architecture is one of the best architecture due to combination of different storage cloud	It is a combination of SSA+BFT.	It provides security and client-side aggregation.	It does not providing privacy preserving public auditing system. Auditing will reduce verification file at each upload.

VI. MATHEMATICAL MODEL

1] Identify the Users U= {u1, u2, u3….}

Where U is main set of Users like u1, u2, u3…u_n

2] Identify the Set of file data Uploaded by user

F= {f1, f2, f3….f_n}

Where F is set of uploaded files like f1, f2, f3… f_n

3] Identify the Set of Files Downloaded by user

D= {d1, d2, d3….d_n}

Where D is set of downloaded files like d1, d2, d3… d_n.

4] Identify the Set of Hash

H= {h1, h2, h3, h4}

Where S is set of hash h1, h2, h3, h4.

5] Identify Servers

S = {s1, s2, s3, s4….s_n}

Where S is main set of servers

6] Identify the set of file data blocks

B= {b1, b2, b3, b4}

Where B is set of file data blocks b1, b2, b3, b4.

7] Identify set of request for files.

R= {r1, r2, r3….r_n}

Where R is set of request for verification r1, r2, r3… r_n.

8] Identify Set of modified block.

M= {m1, m2, m3, m4}

Where M is set of modified blocks m1, m2, m3, m4.

9] Identify Set of Proof.

P= {p1, p2, p3….p_n}

Where P is set of proof required for proof verificationp1, p2, p3… p_n

10] Identify Set of Keys

K= {k1, K2, k3….k_n}

Where K is set of secrete key required for encryption and decryption K1, K2, k3… k_n

VII. CONCLUSION:

In cloud computing, every concept which is related to resources and services is kept at cloud and will get access of cloud by user as online service. Security issue is crucial in Single cloud and Multi-cloud. In Multi-cloud we have to take care of data and operation Performed on it. from single translate cloud to multi-cloud has security challenges. The solution of security issues in Multi-cloud is that use of data security AES algorithms, The data classification strategies and prevention measurement. And also storage files for security purpose.

VIII. ACKNOWLEDGMENT:

I would like to thank my guide prof.R.B.Rathod. Him guidance made by this work to be completed. I would also like to thank my family and project team members who gave me all the support that I needed.

IX. REFERENCE:

1) Bassano, M. Correia, B. Quarrelsome, F. André and P. Sousa, June 2011, “DepSky: dependable and secure storage in a cloud-of-clouds”, EuroSys‟11:Proc. 6thConf. On Computer systems, pp. 31-46

2) C. Cochin, R. Haas and M. Vocalic, June 2010, "Dependable storage in the Intercloud", Research Report RZ, 378.

3) H. Abu-Libdeh, L. Prince House and H. Weather spoon, 2010,"RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, pp. 229-240.

4) K.D. Bowers, A. Jules and A. Opera, 2009, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, pp. 187-198

5) K.rajasekar, c.kamalanathan, June 2012, “Towards of secured cost-effective multi-cloud storage in cloud computing” Undergraduate Academic Research Journal (UARJ), ISSN: 2278 – 1129, Volume-1, Issue-2. Autonomic and Secure Computing (DASC), IEEE, Sydney, pp. 784-791.M. Young, the Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.