e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

SECURED DATA BY MULTICLOUD STORAGE & MULTI ENCRYPTION TECHNIQUES

Ms. Poonam Samal[*1], Ms. Saloni Surana[*2], Ms. Kimaya Chopada[*3], Ms. Pooja Wanj[*4], Prof. Mahendra Jagtap[*5]

[*1,2,3,4]Department Of Computer Engineering, Pune Vidyarthi Griha's College Of Engineering Nashik, Maharashtra, India, Savitribai Phule Pune University, Pune, India.

[*5]Assistant Professor, Department Of Computer Engineering, Pune Vidyarthi Griha's College Of Engineering Nashik, Maharashtra, India, Savitribai Phule Pune University, Pune, India.

ABSTRACT

The use of cloud system has increased rapidly in almost all organizations. Cloud computing provides many assistances in terms of small cost for data storage. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store delicate data with cloud storage service providers but these providers may be untrusted. Dealing with "single cloud" providerss is expected to become less popular with customers due to risks of service availability, failure and the possibility of malicious attack. So a movement towards "multi-clouds" has emerged recently. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work objectives is to encourage the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Keywords: Cloud Computing, Authentication, Security, Single-Cloud, Multi-Cloud.

I. INTRODUCTION

With the increase in use of cloud services cloud providers should address privacy and security issues as a matter of high and urgent priority. Depend on on a single cloud as a storage service is not a correct solution for a number of reasons; for instance, the data could be captured while being uploaded to the cloud, and the data could be stolen from the cloud easily. There are a number of approaches that have been developed in order to provide a secure data storage relying on the multiple-cloud service models. Through this paper we will study, and evaluate the existing approaches that have been proposed as a solution for multiple cloud storage systems in terms of security, privacy, and integrity. Hence, this paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are measured.

II. LITERATURE REVIEW

As per study it is found that most of the existing cloud service provider works on single cloud architecture. Which having some following limitations.

Sr.	Existing System	Advantages	Limitations
1	Single Cloud Computing	i. Availability of data is maintained.	i. Require high cost. ii. Does not provide flexibility and scalability.
2	Data Storage only with Cryptography.	i. Due to encryption and decryption of data, confidentiality is achieved.	i. Only cryptography does not provide full security. ii. Cryptography does not provide integrity and availability.
3	Data Storage Over Untrusted Networks.	i. If Attacker hacks any one network still he does not retrieve any meaningful data.	i. Secret key get be shared with every user. ii. Losses of data.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

III. PROBLEM DEFINITION

To develop a system through in which user can secure his data by splitting single file data into multiple part & encrypt it with different algorithams then stored it on multiple clouds as per numbers of divided parts count to enhanced more sequirity.

IV. EXISTING SYSTEM

Existing system uses single cloud architecture. All data or files of users get stored onto single cloud. SO there is always risk of data lose. Also only one encryption at cloud end is their. So data decryption is also easy.

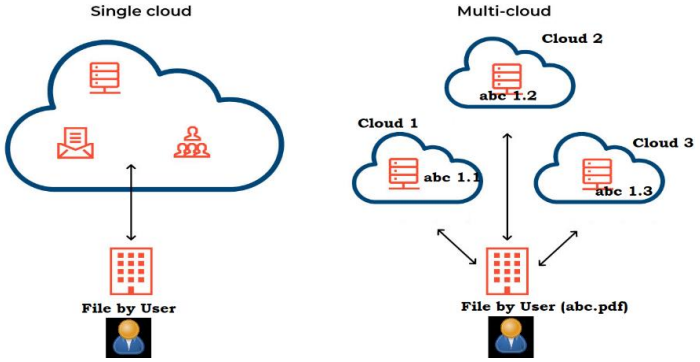

Figure 1: Single Cloud vs Multicloud

V. PROPOSED WORK

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed.

In this paper, an Improved Hybrid Encryption is used to secure the information content data stored in multi cloud. The improved hybrid encryption is the combination of AES, Blowfish and RC5 and ECDH or any feasible encryption algorithm. The data are split up into various number of pieces based on multi cloud resources. And the split pieces are stored in multi cloud using different types of encryption technique. This type of process helps the users to trust the environment. The way of storing files in different cloud are follows. Initially, To make ensure use of multi factor authentication in one form as one time password (OTP). Once the authorized user receive OTP in their registered mail which provides way of primary form of authorized user. Then finding the total sizes in bytes of given data. After that the information data are split into number of parts based on number of cloud service provider. The split pieces are encrypted using different encryption mechanisams.

After the encryption the piece data the directory will be created in each cloud service in the name of the source file. And the encrypted piece data are stored in directory with name as piece number. Each piece of data is stored in different cloud based on the availability of multi cloud. Finally the decryption is the reverse process to merge all data in single information file provide to end user. Finally the files are decrypted according to the request of the authorized user.

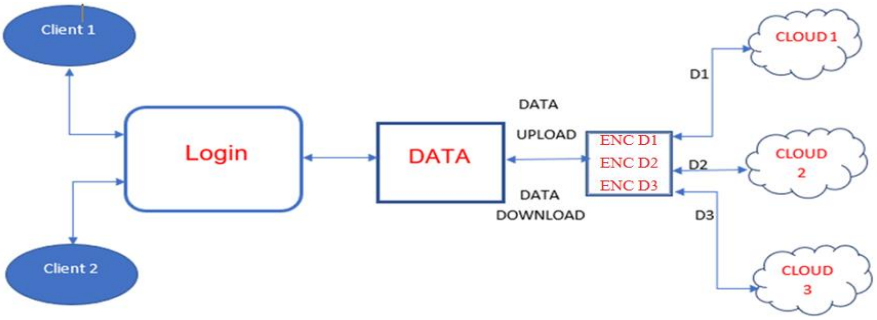

Figure 2: System Overview

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

VI. PROJECT METHODOLIGIES

As per above description main methodologies involved in proposed wirks are :

1. Secure OTP based Login
2. File Spiting & Uploading
3. Data extraction & Encryption (using AES, BlowFish & RC6)
4. Data identification & Decryption
5. File Uploading & Merging
6. Compare the Results

VII. MODULE DESCRIPTIONS & ALGORITHMS USED

For the implementation of proposed multicloud system with more sequrity following modules are devoped.

1. Super User
2. Cloud Owner
3. Cloud User
4. File Splitting & Merging
5. Data Encryption & Decryption

1. Super User

Superuser having overall control on system. He can view all the users information as well as can give approval to file upload and download from all clouds.

2. Cloud Owner

Depending on no. of cloud cloud owners are their. In our work we use five cloud owners. Cloud owners can view name of files & name of users who uploaded file on their cloud. He can view the part of file which is uploade. This information is obiviusly in encrypted format. SO cloud owner cannot view the real data. He having authority to provide access control to uploaded file part once recived the request.

3. Cloud User

Cloud users is a any user who need to use cloud services. This user having facility to uplod his file and aso having functionality to select at list any three cloud from given clouds to store his single file. That means as per selection sigle file get divided into part and each part get uploaded on cloud.

4. File Splitting & Merging

This is a very much impotannt module in which uploaded file by cloud user get divided into three equal parts by using mathematical calculation on file size and no. of data available. When user get access to download uploaded file splitted file get merge and original file will be available for downloading.

5. Data Encryption & Decryption

As per sequrity concern splitted file parts get encryptrd with the help of different encryption techniques and then stored onto multiple clouds. Same way data get decrypted when authentication to download data recived from clouds on which data get uploaded.

VIII. ADVANTAGES OF PROPOSED SYSTEM

1. Data Integrity
2. No any cloud is able to view or store complete data as data get split and then stored each part on different cloud.
3. Sequirity point ov view more reliable.
4. Complex algoritham at each cloud to encrypt data so data decryption is tough for auauthorized users.

IX. DIADAVANTEGES

1. Need to implement complex Algorithms for more data sequirity.
2. Development cost is more.

X. APPLICATION

- In Military application to share confidential files.
- Any private or public organisation where need to secure files.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

XI. RESULT ANALYSIS

The proposed system provide more secure environment as compare with existion single as well as multicloud syste. This system uses different data encryption techniques for each cloud so it will be more secure. No any cloud owner aware about which encryption technique is used to store particular file on cloud. Each file part encrypted with different algorithams.

XII. CONCLUSION

The goal of the system is to secure important files not only splitting it into different parts but also to encrpt each splitted part with different encryption mechanism. We make it happen and obviously it will provide more tight security than availabe existing cloud systems.

XIII. FUTURE SCOPE

In the future enhancement we will try to provide support to store all types of data in encrypted format.

ACKNOWLEDGEMENTS

We thank Prof. Mahendra Jagtap for their expertise and assistance throughout all aspects of our paper. We would like to show our gratitude to all the authors mentioned in the references for sharing their pearls of knowledge. We are also thankful to all the team members, staff who directly or indirectly helped us in making this all possible.

XIV. REFERENCES

[1] "Cloud Security Algorithms", Er. Ashima Pansotra and Er. Simar Preet Singh University, Jalandhar
[2] "Analysis of Security Algorithms in Cloud Computing", Randeep Kaur, Shri Guru Granth Sahib World University, Fatehgarh Sahib
[3] "Security Issues and Security Algorithms in Cloud Computing", K.S.Suresh, Prof k.v. Prasad, Gayatri institute of Engineering and Technology JangareddyGudem, A.P
[4] A. P Shaikh and V. kaul, "Enhanced security algorithm using hybrid encryption and ECC", IOSR Journal of Computer Engineering (IOSRJCE).
[5] A New Approach In Multi Cloud Environment To Improve Data Security 2017 International Conference On Next Generation Computing And Information Systems (ICNGCIS)
[6] Multi Cloud Storage Using Split Algorithm International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET) Volume 6, Issue 3, March 2017, ISSN: 2278 – 1323
[7] Future of Cloud Computing Architecture, Naresh Ramamurthy. Avva Computer Science Department. San Jose State University. San Jose, 95192 669-300-8343 naresh.avva@sjsu.edu.