International Journal of Engineering Technology and Management Sciences[IJETMS]

Website: ijetms.in Issue:2, Volume No.2, July-2018 ISSN: 2581-4621(Online)

Data Partition Technique for secure data storage in cloud using Cryptographic Technique

S.Manjula[1], P.Jothi Thilaga[2],

Department of Computer Science and Engineering, Ramco Institute of Technology,Rajapalayam

[1]manjula@ritrjpm.ac.in
[2]jothithilaga@ritrjpm.ac.in

***Abstract*— Cloud computing is becoming more and more significant for delivery of services and storage of data on the Internet. Cloud storage system allows storing of data in the cloud server efficiently and permits user to access cloud resources without the problem of local hardware and software management. In the cloud atmosphere, resources are pooled among all of the servers, users and individuals. So it is hard for the cloud provider to ensure file security. As a result, it is very easy for hacker to alter and destroy the original form of data. Data security is the main problem. The objective of the project is to overcome security issues by data partition technique. Cloud Manager (CM) is in charge for partition technique. Meta Cloud Manager (MCM) has to retrieve the user file from cloud storage environment. The cloud Manager has possible to view the content of the file. So the Advanced Encryption Standard (AES) algorithm is applied to client data before giving to Cloud Manager.**

***Keywords*— cloud computing, data partition, AES, cloud security, cloud manager, Meta cloud manager**

I. Introduction

The successful evolution in cloud computing over the past few years has managed to a situation that is common to many inventions and new technologies Internet is the key thing for a cloud service, in the sense the services are provided over the internet all over the world. The Cloud Computing technology is embedded with three types of services which are Infrastructure-as-a-Service, Software-as-a-Service and Platform-as-a-Service.These types of services are easy to use and pay as you use. Cloud storage is a service for developers to store and right to use data in cloud. Cloud service provider will be able to and control the cloud resources. Client uses the client devices to contact a cloud system via World Wide Web. The profits of the cloud storage are flexible with compact cost and they also manage the data loss danger.

The Cloud allows users to use a bulk of software and hardware as well as data resources for their applications and services [1]. Public cloud increased to 92% in 2018 from 89% in 2017 and private cloud adoption increased to 75% in 2018 from 72% in 2017 [2]. These recommended that cloud computing is a hopeful platform. However there are several important challenges in securing cloud infrastructures from different types of attacks.

In Cloud computing, both files and software are not completely controlled on the user's computer. File security [7] problems arise because both user's application and program are being located in provider sites. Cloud user privacy is a most important issue in cloud. Some cloud users are satisfied with the current security features while others are afraid about their secrecy. Services based on cloud computing technology let users to store large files or utilize software on a server run over the internet. One in five persons stored files on internet servers [11]. While cost and simplicity of use are the two foremost well-built profit of the cloud computing, there are some major disturbing issues that need to be disables when moving serious application and sensitive data to public cloud.

In this proposed work AES algorithm is used for encrypting the file before giving it to CM. The manager has the duty of splitting the file over the cloud server. The main contributions of this work are

- Promise the secrecy of user data on the cloud through cryptography technique.
- The attacker cannot be opened any meaningful information in the cloud server.
- User data cannot be viewed by cloud service provider as the secrecy of data is maintained by cryptographic methods.

- Availability, reliability and performance of data are improved by replication methods.
- MCM helps to improve the retrieval time of data.

The rest of the paper is structured as follows. Section II delivers an outline of the related work in the field. Section III conveys the proposed approach. Section IV presents an experimental details of our proposed solution. Lastly, conclusions and future work are discussed in Section V.

II. Associated Work

Cloud computing is a developing technology that is going up fast day by day. Cloud computing system is not secured model because there are some security issues and problems. The security is provided to the information which is stored on cloud by using cryptography algorithms. Several investigators studied security challenges and proposed various mechanisms related to Cloud computing models. In this section, we conducted a brief study of correlated work done. In the cloud environment, resources are pooled among all of the servers, users and individuals [13]. So it is hard for the cloud provider to make sure file security. As a outcome it is very easy for an intruder to access, misuse and destroy the original form of data. Reema Gupta et al proposed the file security model which uses the concept of hybrid encryption scheme to obtain security needs [3].

Security issues in three deployment models are discussed by [5].Solutions related with altering, loss and stealing, privacy and control, physical access, data confidentiality, trusting computation are discussed by Abhinay B et al [8]. Security is an necessary parameter and the cloud service provider must verify that there is no unapproved access to the sensitive data of an enterprise during the data transmission [9].Chia-Wei Chang, Pangfeng Liu, Jan-Jan Wu suggested Probability-Based Cloud Storage that selects cloud service providers based on charge and accessibility metrics [6]. File security [4] concerns arise because both user’s application and program are belonging to in provider places.

This paper presents a file security to provide an efficient solution for the basic problem of security in cloud background. In this model, encryption is used where files are encrypted by AES together with file splitting.

III. PROPOSED WORK

The proposed system consists of two modules. It includes Encryption module and Data Partition module.

A. *Encryption Module*

The content of the file is encrypted before giving to CM. For encryption, AES is used. The AES is the encryption algorithm by NIST to replace DES. It is a symmetric-key block cipher algorithm. The AES algorithm has 3 fixed 128-bit block ciphers with cryptographic keys, i.e. 128 bits, 192 bits and 256 bits. The size of the key is unlimited, where the block size is maximum 256 bits. AES encryption technique is fast, flexible and secured. It can be supported on various platforms [12]. The proposed system is described in Figure-1.

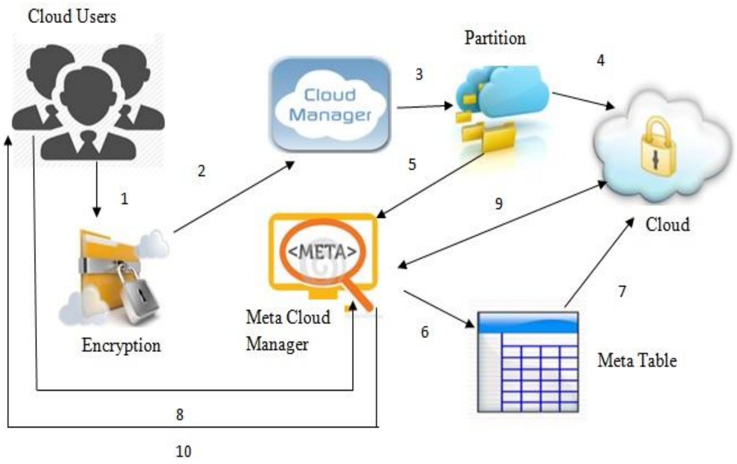


Fig.1. Proposed System

The proposed work includes the following 10 steps for file upload and download.

Step 1: An authenticated user enters for file upload in the cloud.
Step 2: The file is encrypted using AES.
Step 3: Encrypted file is splitted by CM.
Step 4: Splitted file is placed on cloud storage by CM.
Step 5: Location of the splitted file is given to MCM.
Step 6: MCM stored it in Meta table.
Step 7: Meta table is uploaded in cloud storage.
Step 8: Downloading of files will be done only by the authenticated user after verifying of cloud registration details and user directed to MCM.
Step 9: MCM retrieved file from cloud.
Step 10: An authenticated user finally get the original file.

B. Data Partition

Data partition is a process of splitting the file into several parts. Data that has been partitioned down can be recollected as a whole. To improve cloud data storage security, the proposed work uses Data Partitioning Technique. The major components of the proposed work are,

1)Cloud Users

An entity or person upload data to be store and retrieve from cloud storage and relies on the cloud for data storage and computation.The file E(F) is uploaded by cloud user has encrypted file.

2)CM

The CM has responsible for fragmenting the E(F) and replicating the E(F).The algorithm used for splitting by CM is shown as Algorithm 1.

3)MCM

The MCM has responsible for storing meta table in cloud storage and retrieve the data from cloud storage.

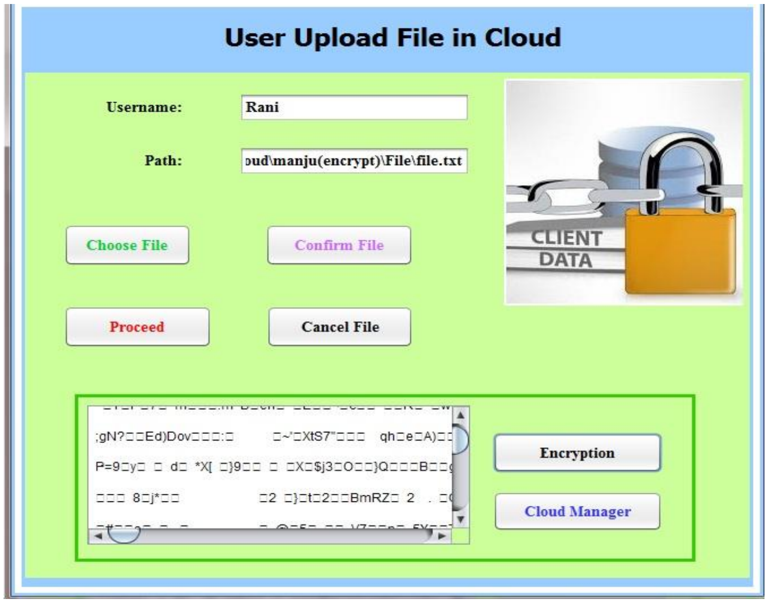
C.Data Partition algorithm

```
1. Get the input file E(F).
2. Find the number of lines l in the E(F).
3.If
        E(F)<=min size or size>=max size
    show error message.
Else
        Partition file as per the threshold value fixed.
```

Consider if F^a denote the a th fragment of file F.f^a represents the size of F^a. F^a be calculated as probability that n number of lines in F. The F is split using the optimal threshold value. The probability of getting the content of E(F) be minimized here. This will show that if attackers have a chance to attack cloud server he may not be able to get valuable data.

IV. IMPLEMENTATION RESULTS

Using JAVA and MegaCloud storage the proposed work was done. In this section the implementation of the proposed work was done. In Figure-2, the registered user is provided to pick a file and encrypt the content. Finally the encrypted file is moved to the CM.



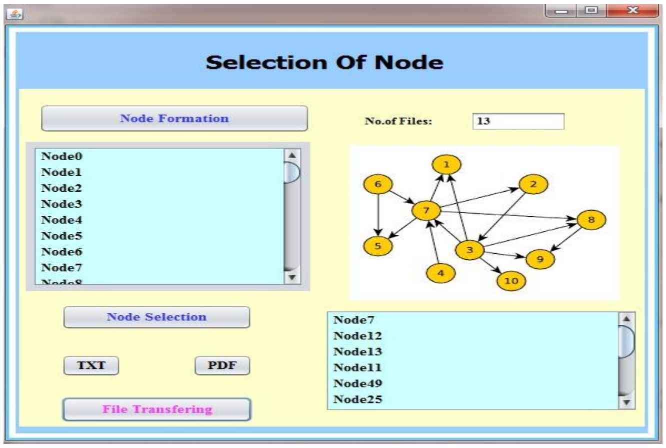
Username: Rani

Path: oud\manju(encrypt)\File\file.txt

```
;gN?□□Ed)Dov□□□:□      □~'□XtS7"□□□  qh□e□A)□□
P=9□y□ □ d□ *X[ □}9□□ □ □X□$j3□O□□}Q□□□B□□
□□□ 8□j*□□             □2 □}□t□2□□BmRZ□ 2  . □
```

Figure.2. File upload

In Figure-3, CM progress the encrypted file by creating the several nodes and distribute the split content of the encrypted file in randomly chosen nodes.



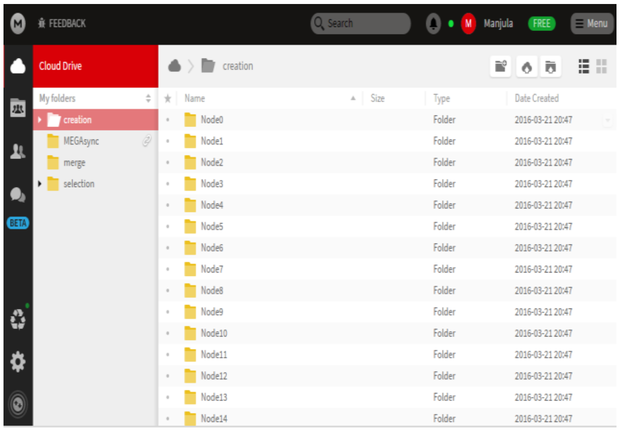
No.of Files: 13

```
Node0
Node1
Node2
Node3
Node4
Node5
Node6
Node7
```

```
Node7
Node12
Node13
Node11
Node49
Node25
```

Figure.3. File split

Figure-4 shows that the node is created in the MegaCloud environment.



Name	Size	Type	Date Created
Node0		Folder	2016-03-21 20:47
Node1		Folder	2016-03-21 20:47
Node2		Folder	2016-03-21 20:47
Node3		Folder	2016-03-21 20:47
Node4		Folder	2016-03-21 20:47
Node5		Folder	2016-03-21 20:47
Node6		Folder	2016-03-21 20:47
Node7		Folder	2016-03-21 20:47
Node8		Folder	2016-03-21 20:47
Node9		Folder	2016-03-21 20:47
Node10		Folder	2016-03-21 20:47
Node11		Folder	2016-03-21 20:47
Node12		Folder	2016-03-21 20:47
Node13		Folder	2016-03-21 20:47
Node14		Folder	2016-03-21 20:47

Figure.4. File split in cloud environment

V. CONCLUSION AND FUTURE WORK

The proposed work uses a partition of data into splits. Partition of data in the cloud helps to protect files from hackers in seeing entire file. And also even if the hacker saw the file stored, he may not see which part of file it is and also he cannot know what data it contains as it is encrypted. The encryption of file using unbreakable algorithm and split of the file ensures data privacy. The future work is store split data on multiple cloud service providers to enhance data security and to avoid failure of data by replication technique.

REFERENCES

[1] J. Che, Y. Duan, T. Zhang, J. Fan," Study on the security models and strategies of cloud computing",Procedia Engineering, Vol. 23,pp586-593, 2011.

[2] www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2018-state-cloud-survey.

[3] Reema Gupta,Tanisha, 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.

[4] Akhil Behl, "Emerging Security Challenges in Cloud Computing", in Proc. of World Congress on Information and communication Technologies ,pp. 217-222, Dec. 2011.

[5] AnujKumarYadav, Ravi Tomar, Deep Kumar and Himanshu Gupta," Security and Privacy Concerns in Cloud Computing" in International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 5, May 2012.

[6] Chia-Wei Chang, Pangfeng Liu, Jan-Jan Wu, "Probability-Based Cloud Storage Providers Selection Algorithms with Maximum Availability," icpp, pp.199-208, 2012 41st International Conference on Parallel Processing, 2012.

[7] Akhil Behl, "Emerging Security Challenges in Cloud Computing", in Proc. of World Congress on Information and communication Technologies ,pp. 217-222, Dec. 2011.

[8] AbhinayB.Angadi, AkshataB.Angadi, KarunaC.Gull,"Security Issues with Possible Solutions in Cloud Computing-A urvey"inInternational Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[9] Kan Yang, XiaohuaJia, " Attributed-based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2011.

[10] Ahmed Lounis, Abdelkrim Hadjidj,AbdelmadjidBouabdallah, YacineChallal, "Secure and Scalable Cloud-based Architecture for e-Health Wireless sensor networks", 21st International Conference on Computer Communications and Networks (ICCCN), Munich, 30 July -2 Aug 2012, pp 1-7, Print ISBN: 978-1-4673-1543-2.

[11] http://ec.europa.eu/eurostat/statistics-explained/

[12] "Analysis of security algorithms in cloud computing", International journal of invocation in engineering and management(IJAIEM), Student Masters Of Technology, Shri Guru Granth Sahib World University.

[13] Sonia Verma and Amit Kumar Chaudhary "Save and secure data on clouds" journal of global research in computer science,vol 5,no 4,2014.