International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

SPLIT AND COMBINER METHOD OF CRYPTOGRAPHY FOR CLOUD STORAGE SECURITY

Mr. V Vivekanandan[1], Mr. R Suresh Kumar[2]

Assistant Professor, Department of Computer Science and Engineering
KGiSL Institute of Technology, Coimbatore, India

Abstract- Cloud storage it is a model for computer data storage when the digital data gets stored in the logically pooled storage devices. There are many online storage providers like Google Drive, Box, OneDrive, iCloud, Dropbox, Amazon drive and so on. Every cloud storage providers have security mechanism to prevent data from hack hackers but still we have some issues in security to resolve that we have an idea to split the data into multiple segments each segment is encrypted using different encryption algorithms then each segment is stored in different locations of cloud storage then again while retrieving data we have to decrypt by its algorithm then combine the various segments from different locations then we will get the actual data after integration. In this case we can avoid security issues in cloud storage.

Keywords- Cloud, Splitter, Combiner, Encryption and Decryption.

I. INTRODUCTION

Nowadays cloud storage is attracted everyone to store the data in cloud storage and we can retrieve our data from Cloud anywhere using any device with internet connection. It is easy to maintain our data in cloud and it is secure when our data get lost in any disaster we can recover our data from replication server. There is a security mechanism for data recovery when data lost but there is an issue in providing security mechanism to protect data from intruders and hackers.

All know that cloud is secure if it is secured then how Apple's iCloud hacked. Once it is hacked then immediately there is a drop in the popularity of cloud storage. Consumers are always demanding quality, security and availability. If these things are maintained correctly then we can bring the popularity of cloud storage to higher level.

There are some best cloud storage platforms like Drop Box, Google Drive, One Drive and Box. These are the nest cloud storage platform in current trend and every one using it. But there is some security issue when we store our data in the third party side. So there is need of mechanism to improve the security in cloud storage and working on it to deliver the good quality and secured cloud platform for the data storage.

II. PROPOSED SYSTEM

In current scenario data size increasing dramatically so in local machine we can't accommodate that kind of data, in that case we are in demand to use of scalable storage space. So we will go for the technology called cloud computing. In some cases there is an security issue in cloud storage because our data is getting stored in the third party server and also data is replicated in multiple location for data recovery. Data is safe from any kind of disaster but data is not protected from intruder and hacker. To avoid this kind of issue now we go for the split and combiner method of cryptography for cloud storage security. In this method consumer actual data is split into three segments, every segment is encrypted using different encryption algorithm then encrypted data is stored in the different location. Encrypted segment 1 stored in location 1, Encrypted segment 2 stored in location 2 and Encrypted segment 3 stored in location 3. Here location indicates the various data center or server in different location in which our data gets store. So data will be more secure from hacker. In case hacker hacked data means they will get only one part of the data that will be in encrypted form which is not understandable. Suppose that segment is decrypted by hacker means also our data will be secure because another part of data is in another location which is not discoverable by hacker. Data flow and workflow is defined in architecture diagram.

Algorithm Selection

From reference paper "Survey on Various Data Encryption Algorithms Used in Cloud Security" in "International Journal of Innovative Research in Computer and Communication Engineering" the symmetric encryption algorithms Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES)are considered to be best encryption algorithm for cloud storage security.

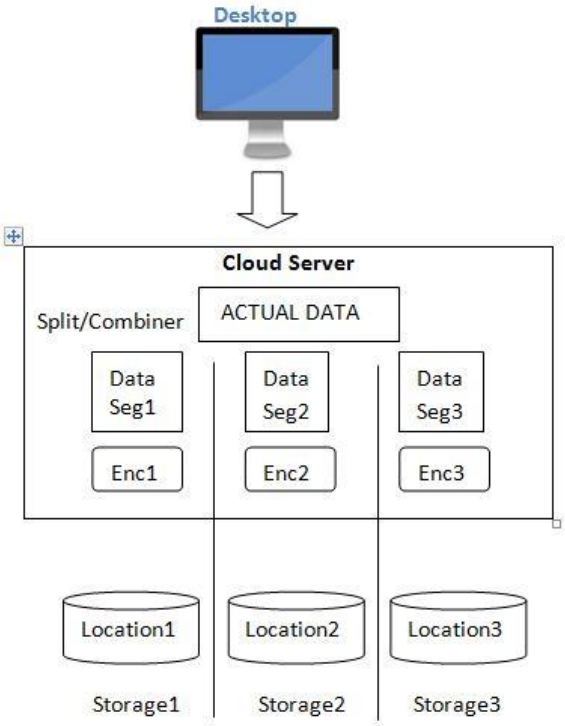


Figure 1: Secure Cloud Storage Architecture

III. MODULES

1. Splitter/Combiner.
2. Encryption/Decryption.
3. Storage in different location.

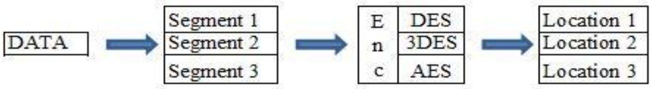
Splitter/Combiner

The actual data receive from the user to store in cloud storage, it splits into three segments and name it as segment 1, segment 2 and segment 3. While data storage in cloud it splits data and sends to the next level to perform encryption. In the process of data retrieval it will get decrypted data from decryption module and it combines or integrates the three segments of data together to make actual data for users need.

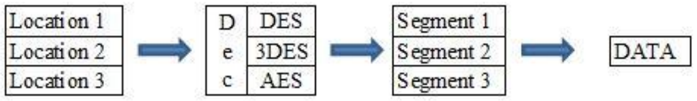
Encryption/Decryption

Each split data segment is encrypted using different encryption methods. For example segment 1 is encrypted using DES, segment 2 is encrypted using RSA and segment 2 is encrypted using AES. Have to avoid using same method in different segments. Each segment should use different encryption methods. While user retrieving or data access from cloud it will fetch encrypted data from different locations then using same method it will decrypt to get the actual data.

Encryption and store Data



Decryption and Retrive Data



Storage

In storage part the segment of encrypted data is get stored in various location. Each segment will get store in different location. Then while users access data it will retrieve data from various location and sends to the decryption module.

IV. CONCLUSION AND FUTURE ENHANCEMENT

Here cloud storage platform is secured by the way of using split and combiner method of cryptography for cloud storage platform security. In Future there is an improvement in choosing the optimized way of using the encryption and decryption algorithm by considering some parameters. Choosing the right locations for storing the data should be optimizing in the next future for improving the performance of cloud storage and also to protect data.

REFERENCES

1. https://www.bbc.com/news/technology-29237469
2. https://systemsandsoftware.com/5-safety-concerns- with-cloud-data-storage-answered/
3. Nisha D. Dable, Nitin Mishra, "Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment" IRD India Volume -3, Issue -4, 2014.
4. Mr P.Madhavan, M.Anitha, P.M.Dhravya, N.Keerthana, "MULTI CLOUD STORAGE USING SPLIT ALGORITHM", IJARCET, Volume 6, Issue 3, March 2017, ISSN: 2278 – 1323.
5. Rohit Bhore, Dr. Rahila Sheikh, "Secure Data Storage Scheme Using Cryptographic Techniques in Cloud Computing", IJCSN International Journal of Computer Science and Network, Volume 5, Issue 1, February 2016.
6. S.Sandhya, U.Reshma, Dr.V.Praveena, "Survey on Various Data Encryption Algorithms Used in Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 9, September 2017.

AUTHOR'S BIOGRAPHIES

Mr. Vivekanandan V ME.,

Work Experience:

- Software Test Engineer with Foreview Technologies Pvt Ltd, Coimbatore since Feb 2015 to Till Date.
- Eight month work experience in Educomp Solutions Ltd (ERP Management in Academic Support). From December 2012 to August 2013.
- Six Month work experience in Ugam Solutions Ltd as Consultant. From June 2012 to December 2012.

Paper Publications:

1. "BIG DATA ANALYSIS TO INCREASE EFFICIENT PERFORMANCE OF DATA". In Proceedings of International Conference on Adaptive Technologies for Sustainable Growth organized by Pavai Engineering College, Namakkal.
2. "EFFICIENT DATA ANALYSIS SCHEME FOR INCREASING PERFORMANCE IN BIG DATA" IJAICT Volume 1, Issue 2, June 2014
3. "CREATING DATA BACKBONE FOR STUDENT BEHAVIOR ANALYSIS USING DECICION SUPPORT SYSTEM", IJAICT VOLUME 1, ISSUE 8, DECEMBER 2014