DOI 10.29042/2018-4019-4023

Helix Vol. 8(5): 4019- 4023

Multi-Cloud Based Secured Storage System

[1]M.V.Bramhe, [2] Dr. M.V.Sarode
[1]PhD Scholar, GHRCE, Nagpur
[2]Professor, Government Polytechnic, Yeotmal
Email: manoj_bramhe@yahoo.com

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract
Present days' cloud computing has become successful computer paradigm because of "pay-as-you-go" model. Various solutions were proposed for handling cloud vulnerabilities and threats but most of which concentrate on single cloud environment which faces many problems like malevolent system administrator, service failure, loss of data integrity and data intrusion problem which can be reduced by moving towards multiple cloud environment. This paper mainly focuses on techniques for reliable secured storage in Multi-cloud environment by securely deploying chunks of data in multiple clouds where adversary will never get complete data at one place.

Keywords: Multi- Cloud, Inter Cloud, SaaS, PaaS

Introduction

Cloud Computing is much popular for big and small organization because of its "pay-as-you-go" nature which has reduced operational and implementation cost. Cloud Computing is defined by NIST as model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. It consists of 5 essential characteristics, three delivery models and four deployment models [1].

Many solutions were proposed for single cloud based environment to maintain cloud storage security bur it faces various issues like malicious system administrator, data integrity loss and data intrusion problem, failure of service, untrusted cloud provider which can be removed by shifting from single to multi cloud environment [7]. It is noted that around eighty percent research was carried on single clouds whereas only 20 percent research was done in multi-clouds [4]. User data is divided into multiple chunks and stored on various clouds in inter / multi cloud environment which eliminates all these threats as malicious user never get a complete data set.

We have proposed secured storage in Multi-Cloud environment where reliable and scalable data storage is created using cryptographic functions by uploading user's data in multiple clouds.

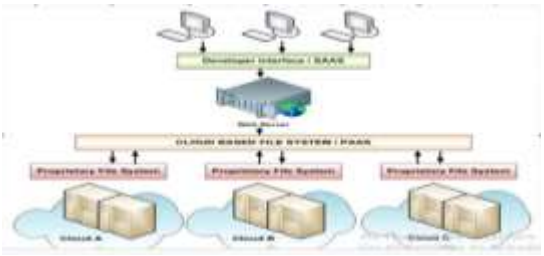

Figure 1: Proposed System Architecture

Our proposed system allows the user to upload data to multiple clouds randomly chosen by the system or as per manual selection by the user. The data is uploaded in secured way by encrypting it before or after splitting into three parts. These parts are stored in three different public clouds. Once verified, multiple chunks are merged to generate original data of the user.

Our technique supports variety of private key algorithms which not only secure data but also makes simple and fast system due to less computation involved. The keys of user are not stored in cloud but in a local server which will make them secure as nobody knows the keys generated other than the owner.

Related work

Mohammed A. Alzain et al. in [4] described multi-cloud model as combination of various clouds where user data will be distributed and executed simultaneously. It is observed that multi–cloud system improve performance provided by single cloud environment by dividing security, trust and reliability among different clouds. They have made a survey of various techniques available for multi cloud security like use of cryptography, secret sharing algorithm, DepSky system, redundant array of cloud storage (RACS) and HAIL protocol. Bohli J. et al. have proposed 4 different architecture for multi-cloud computing paradigm for improving security and privacy of user and provider [6]. Various architectures have their advantages and disadvantages but we can get better model for multi-cloud environment by combination of those architectures. In [16] a revised lakely's secret sharing mechanism is proposed to improve security and reliability of DFS without affecting scalability. This scheme does not require key management .To reduce computation overhead in this scheme, Graphical processing unit is used. Fan-Hsun et al. proposed secure and reliable cloud DFS using

replacement of Hadoop DFS with open source based Tahoe least-authority file system [17]. Kheng Kok Mar in [19] introduced multiple cloud based secure virtual diffused file system by hosting it on exiting setup of public cloud. Our techniques are similar

Proposed System

Proposed system is divided into two main modules for uploading and downloading of data to multiple clouds. Secure uploading to multiple clouds is carried by splitting original file into multiple chunks and uploading it securely using encryption. Downloading of the chunks and merging it to create original file is carried after verifying user credentials.

File Split Module

This module is used to divide file to be uploaded into multiple chunks. User has 3 options to split file. Option 1is to split file in 3 parts without encryption, used by the user who do not want any security measures from the system. The users who wishes total secure uploading to clouds can have it in 2 ways either encrypting file before split or after split. User can choose any private key security algorithm for encryption. Currently we have provided AES and DES algorithm. The details of the process is shown in the figure no.2 below

Figure 2: File Split

Upload Module

Upload module is used to securely upload the data in multiple clouds as shown in the below figure

User data is uploaded to clouds as per steps mentioned below.

Step1: User Ui submits authentication details to cloud Authorization module

Step2: Cloud authorization module validates authenticity of the user and allows him to upload data

Step3: User submit data which can be uploaded to clouds by 2 different way

Step3.1: If user chooses to encrypt the data before split then user has to chooses private key algorithm for encryption along with random key

Step3.1.1: Encrypted data is submitted to split & upload module which will divide it into 3 chunks and upload those chunks in 3 different public clouds

Step3.2: If the user chooses to split the data before encryption then it will be divided into 3 chunks

Step3.2.1: Spitted data is encrypted as per chosen algorithm and random key and then uploaded to multiple clouds Metadata is created during the process so that it will be helpful to manage and merge multiple chunks

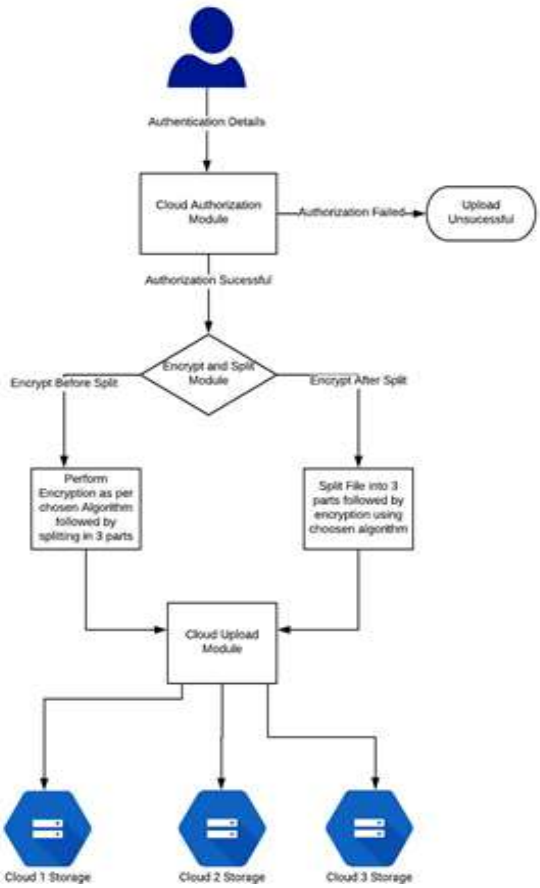

Figure 3: Upload Data

Download Module

Download module is used to download the required data securely from multiple cloud, merge them in original form for the user.

User data is downloaded from multiple clouds as per the steps mentioned below

Step1: User Ui submits Data / File name to be downloaded along with user authentication credentials

Step2: Cloud authorization module verifies user authentication. If not verified then system will not allow them for data download

Step 3: If the user authorization is successful then system will download multiple chunks from multiple clouds where data is uploaded

Step3: All downloaded chunks related to user are merged together to generate original data requested by the user
Step4: User is allowed to download data requested from cloud system to local drive as per the location chosen by him.

Metadata created during uploading of data is used to map the various

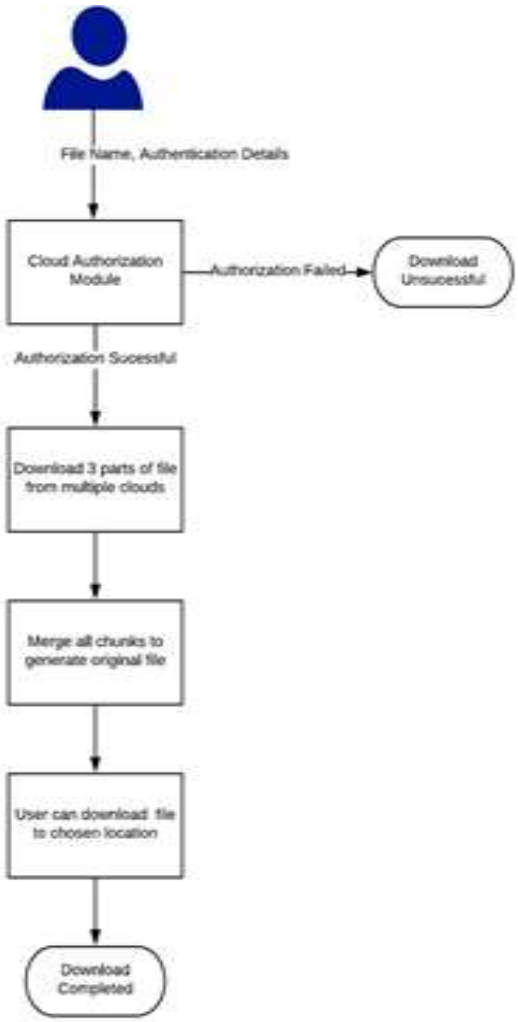

Figure 4: Download data

Results
The system is tested on local and cloud based environment. Two scenarios were used for unsecured storage on cloud without encryption and secured storage with basic encryption methods of AES and DES cryptographic algorithms. Different options were provided to the user for splitting the file before or after encryption process. System used is Pentium i3 server with 2GHZ quad core processor and 4 GB of RAM.

Following Screenshot shows the actual upload process to multi-clouds. Data is divided into 3 different size chunks and uploaded to various clouds securely by encrypting them before or after split.
Total time required to upload data is mentioned which depends on network bandwidth and configuration of server.

Figure 5: Multi-Cloud Upload

Cloud environment has access to the user's data. AES is most secured and efficient private key cryptographic algorithm. System is reliable as it can always get back original data during the failure of one of the cloud services using RAID like techniques.
Secured storage is obtained using multiple clouds as data is deployed in various clouds and adversary will never get complete set of data.
Downloading of the desired file is easy process with user authentication as initial phase for confirming user credentials before downloading desired data. Download is rejected for failed user authentication and accepted for successful one. The following screenshots shows download process from three clouds. User will provide original name of the file to be downloaded along with primary key which will be used to download 3 different chunks from 3 cloud services and merged together to generate original file. User can confirm the successful merging of chunks from various cloud by comparing size of the downloaded file with original file uploaded before splitting.

Figure 6: Multi-Cloud Download

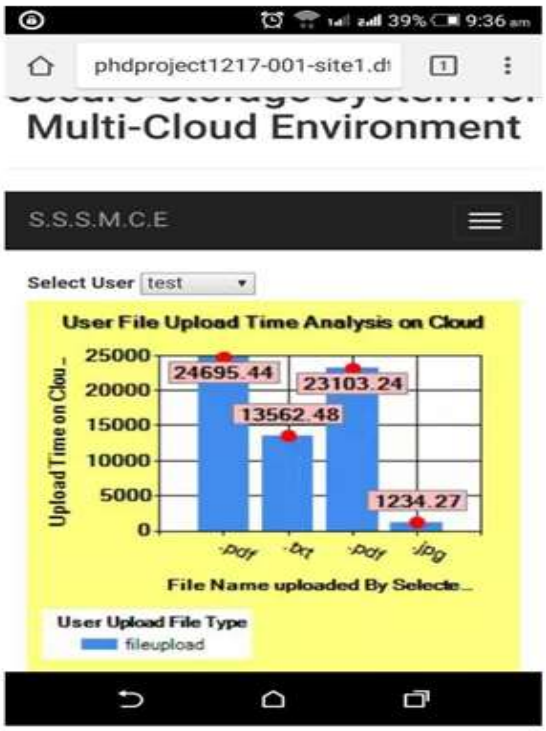

Figure 7: Upload Time Analysis

The system is tested on local and multiple clouds for various types of files like .doc, .pdf, .txt. jpg, .bmp as well as audio and video files . Different size of files ranging from KBs to several MBs are uploaded and downloaded successfully. Figure 7 shows upload time analysis graph for four different types' of files .Time mentioned is in millisecond. Required time for uploading and downloading of files is dependent on the configuration of local system along with the internet bandwidth.

Conclusion

The system is implemented for secured storage using Multi-cloud environment. System uses cryptographic Encryption algorithm for secure uploading of the multiple data chunks to various private or public cloud Services. User data can be retrieved successfully by downloading and merging chunks from multi clouds after successful user authentication.

Even though very less work is carried out in multi-cloud environment than single cloud but it is observed that in multi Cloud based systems user data is fragmented among various private / public clouds so that adversary cannot get complete set of data at a time Which removes most of threats occurring in single cloud environment.

References:

[1] Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas DRAFT Cloud Computing Synopsis and Recommendations, NIST Special Publication 800 146, May 2011

[2] Cloud Security Alliance (CSA). "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," (Released December 17, 2009), http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[3] Zhifeng Xiao and Yang Xiao, "Security and PrivacyinCloudComputing",IEEE Communications Surveys & Tutorials, March 2012

Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE 45th Hawaii

International Conference on System Sciences, 2012

[4] Singhal M., Chandrasekhar S., Tingjian Ge., Sandhu R., Krishnan R., Gail-Joon Ahn., Bertino E., "Collaboration in Multicloud Computing Environments: Framework and Security Issues", IEEE computer society journal, Vol. 46, Issue 2, pp. 76-84, Feb 2013

Bohli J., Gruschka N., Jensen M., Lo Iacono L., Marnau N, "Security and Privacy Enhancing Multi-Cloud Architectures," IEEE Transaction on Dependable and secure computing, Vol PP, Issue 99, 2013

[5] Tran Doan Thanh, Subaji Mohan, Eunmi Choil, SangBum Kim, Pilsung Kim "A Taxonomy and Survey on Distributed File Systems," IEEE Fourth International Conference on Networked Computing and Advanced Information Management, 2008

Paval Bzoch, Jiri Safarik, "Security and reliability of distributed file systems," 6th IEEE international con. on intelligent data acquisition and advanced computing systems, Sep 2011

[6] Dalibor Peric, Thomas Bocek, Fabio Victora Hecht, David Hausheer, Burkhard Stiller, "The design and evaluation of a distributed reliable file system," Int. Conference of parallel and distributed computing, application and technologies, 2009

[7] Jumpei Arakawa, Koichi Sasada, "A decentralised access control mechanism using authorization certificate for distributed file systems,"

6th Int. Conference on internet technology and secured transactions, UAE, December 2011

[8] Hung-Chang Haiao, Hsueh –Yi Chung, Haiying Shen, Yu-Chang Chao, "Load rebalancing for distributed file systems in clouds," IEEE transactions on parallel and distributed systems, Vol. 24, No. 5, May 2013

[9] Hadoop Distributed File System, http://hadoop.apache.org/hdfs/2012

[10] Satyanarayanan, M., "A Survey of Distributed File Systems," Technical Report CMU-CS-89- 116, Department of Computer Science, Carnegie Mellon University, 1989

[11] Sandesh Uppoor, Michail D. Flouris, Angelos Bilas, "Cloud-based synchronization of distributed file system hierarchies," IEEE , 2010

[12] Paval Bzoch, Distributed File Systems, Technical Report no. DCSE/TR-2012-02, University of West Bohemia, June 2012

[13] Su Chen, Yi Chen, Hai Jiang, Laurence T Yang, Kuan-Ching Li, " A secure distributed file system based on revised Blakely's secret sharing scheme," 11th IEEE international conference on trust, security and privacy in computing and communications, 2012

[14] Fan-Hsun Tseng, Chi-Yuan Chen, Li-Der Chou, Han-Chieh Chao, "Implement a reliable and secure cloud distributed file system," IEEE international symposium on intelligent signal processing and communication systems, November 2012shna Kant, "Enhanced Distributed storage on the cloud," IEEE 3rd nternational conference on computer and Communication technology, 2012

[15] Kheng Kok Mar, "Secured virtual diffused file system for the cloud," 6th International IEEE conference on internet technology and secured transactions, UAE, December 2011

[16] Kim-Kwang Raymond choo, omer F. Rana, Muttukrishnan, "Cloud Security Engineering: Theory, Practice and future research," IEEE Transactions on cloud computing, Volume 5 Issue3, 2017

