International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Implementation of Secure Multi Cloud File Storage

Yogita M Pattan, Peruru Vanaparthi Sai Likhitha, Prof. Raghavendra Prasad, Prof. Smitha G R

Department of Information Science and Engineering, RV College of Engineering
R V Vidyaniketan Post, Mysore Road, Bengaluru - 560 059, Karnataka, India

---

Abstract - *Data security is one of the major concerns in Information Technology, particularly in Cloud Computing. When it comes to Multi-cloud storage, it is also very important to maintain Data Integrity across the cloud servers since they may be located anywhere around the globe. One cannot ignore the threats to a user's data on cloud even though cloud provides wide range of services like storage capacity, cost savings and high speed. Enterprises and businesses use cloud services to store their files, but this exposes confidential and sensitive file to new risks. The proposed Multi-cloud storage provides a secure mechanism for file storage by abstracting the process of storing files across multiple servers to the users and enhancing the security and privacy of data with a trustworthy environment. The user of the cloud need not worry about the way data is stored in multi cloud servers or about the way it is uploaded or downloaded. The methodology adopted ensures the integrity of data in files is maintained when the data is retrieved by the user. This paper describes the implementation of a secure Multi-cloud storage for files by adopting encryption and file splitting concepts to improvise the security of file stored. Here, the user's file is fragmented into segments and each segment is loaded into a different cloud server. The files parts are encrypted by making use of keys unique to each cloud server before being loaded. Double encryption is provided when the user first encrypts the file before it can be uploaded to the cloud server and the integrity is ensured by hashing each file part before encryption. All the metadata corresponding to a file's fragmentation and encryption is maintained by a combiner module. The suggested model ensures both Data privacy and security, and Data Integrity.*

Key Words: **Multi-cloud storage, File security and privacy, Data Integrity, Cloud computing, Encryption, File splitting**

1. INTRODUCTION

Cloud computing provides on-demand and pay-as-you-go availability of system resources in the form of computing power and storage. It is a group of networked elements providing services which is not managed by the users but providers. It saves infrastructure and operational expenditures for organizations due to scalable access over the internet.

Security challenges are amongst the largest obstacles when adopting a cloud service. The delicacy and sensitivity of the user's information is one of the major reasons why the user may hesitate to store this information in the cloud. Organizations and Enterprises hesitate to leverage public cloud services for storing their sensitive and confidential data as some of the clouds store them as plain text on a server which may be located anywhere around the globe making security a concern. These security concerns develop novel ideas and techniques for security approaches. Some cloud services provide the ability to encrypt the data that is to be stored. This raises a security concern when the user has no idea as to who has access to the encryption keys. The cloud administrators may use the keys for malicious activities. Some of the complex data security challenges include sharing the infrastructure of a cloud service model with multiple tenants, legal issues and data mobility, Compliance and auditing concerns, standards adopted by the cloud service providers. Hence, there is a need of a secure method for the user to be able to trust the cloud service in maintaining their confidential data.

Multi-cloud storage is the deployment of multiple cloud services within a single networked architecture. A typical multi-cloud architecture may utilize several public and private clouds which in turn eliminate the reliance on a single cloud provider. They have the potential to allow higher security and performance. In the case of single cloud storage, all the data is stored on a single centralized region which makes it easily accessible to the attackers. Multi-cloud storage is also advantageous in terms of disaster recovery and cost saving. The strategy of multi-cloud allows organizations to select different clouds services based on their advantages over certain tasks than others. Using a multi-cloud environment, the cloud service provider can handle different aspects of security whereas the organizations can define their own security responsibilities over the cloud.

Our proposed system provides a multi-cloud based cloud service which adopts a secure method of storing files in the cloud servers. It involves splitting, hashing and encryption procedures that overall make the storage of files secure across multiple servers. The file is split into multiple parts and stored in different servers such that a malicious attacker never gets complete data even if a cloud server is compromised in turn enhancing the trustworthiness of cloud services. The security is improved by adopting encryption-decryption techniques and data integrity as maintained by hashing the file segments.

This paper is structured as follows. Section II discusses the related work on Multi-cloud file storage. Section III discusses the proposed methodology for secure file storage.

2. RELATED WORK

Majority of the research was executed on single cloud storage services where the entire data is stored on a single location leading to security concerns like data loss, data integrity issues, malicious attacks by cloud administrators. A solution to these was provided in [1] which adopted multi cloud storage to improve the performance. Multi-cloud storage like DepSky, RACS is briefed with their benefits and shortcomings in the paper. A wide range of security domains such as key administration, encryption and identity management are discussed in [2].

Distributed File System (DFS) are leveraged by many of the multi-cloud systems to allocate and store files in a distributed network. Popular DFS are considered in [3] and [4]. Another method described in [5] explains distributing the file data and metadata separately within a single server. Cloud security issues and challenges are discussed by NIST in their draft of Cloud computing synopsis [6]. A proxy re-encryption strategy for data and information sharing is discussed in [7] where the overall security is lessened due to storing the whole file in a single cloud server.

3. PROPOSED METHODOLOGY

The proposed methodology includes a number of modules which perform major operations of storing a file into multiple cloud servers. Every file undergoes processing before it is stored in the file. These are discussed in every step listed in this section.

Step 1: User Login

This is the module where the user logs in to the system. Every user is registered into the system before they can login. Registration is done at the organization level which allows users belonging to an organization the ability to login.

Step 2: Upload and Download

This module provides the user the ability to upload the file to be stored in the cloud server and the ability to download the file from a cloud server. A primary level of encryption is performed here with a key private to the user. This is to guarantee that even the cloud gets compromised somehow attacker would not know the contents of the file. This provides an upper hand to the user.

A user interface would be provided to the user to view the files stored into the cloud and an option to download any file that is stored in cloud. There are no restrictions on the type and number of files a user can upload.

Step 3: Combiner Module

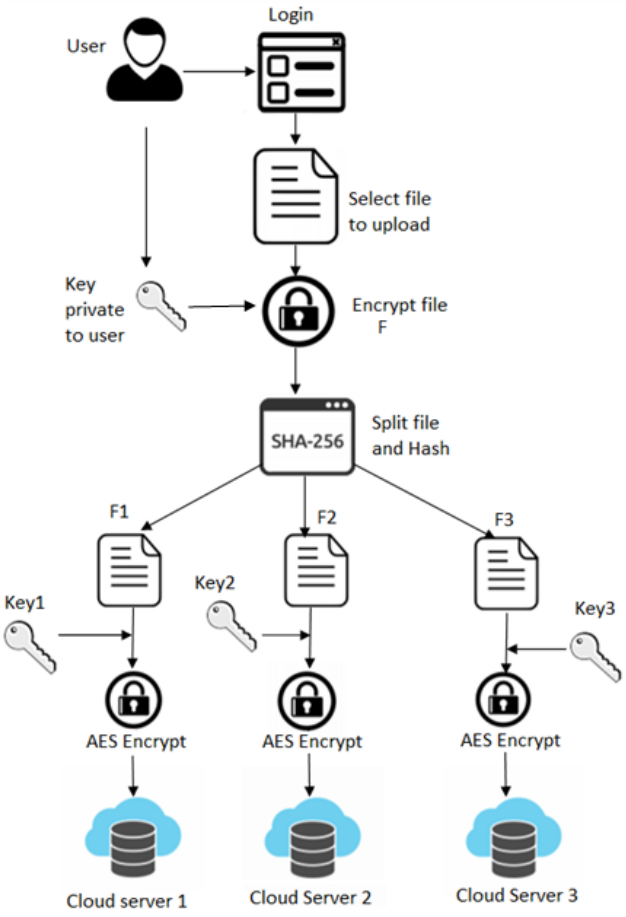

Fig -1: Secure Multi-Cloud File Storage Architecture

This is the module which abstracts the processing done on the file to the user. This module includes two major operations which are performed on the file.

The first step performed by the combiner module is of file splitting. The file selected by the user to be uploaded to server is split into a number of parts based on the number of servers to store the file parts into.

Once a file is fragmented into parts, a signature that is, a hash is generated for each part of the file. SHA-256 is the algorithm used to generate this hash. A hash is a signature for a text which is different from decryption in that it is a one-way cryptographic operation performed on a text. SHA-256 creates a unique 256 bit hash for each part of the file. SHA-256 is one of the strongest hashing functions and has not been compromised.

Hashing provides the following benefits:

1. Data Integrity verification: The file and its parts' data integrity can be verified with the hash generated for each of them. In case a file is tampered, the hash calculated will be different from the hash of the file generated before it was loaded to cloud thus providing information regarding the integrity of content of the file. Once all the file parts are merged, a hash is generated on the complete file and this

hash is compared with the original hash generated before the file was stored in the cloud. If the hash does not match, it proves that the file has been tampered with.

2. File part order verification: The combiner module has information on the order of the files. Once a file to be downloaded from the cloud servers, the combiner module combines all the fragments of the file into one file. The hash generated for this combiner file must be same as the original hash to verify that the file has been merged in the right order

After the files has been split into number of parts, each part of file is encrypted with different key, the key to encrypt that particular part of file depends on which server the combiner module wants to store that file in, that is a key is unique to a sever. These keys are generated by the combiner module and assigned to each server.

Encryption algorithm which has been used to encrypt files is Advanced Encryption Standard (AES) algorithm which is symmetric encryption algorithm, Advanced Encryption Standard (AES) algorithm is basically an iterative approach rather than the Feistel cipher. It is particularly designed to depend on substitution and permutation network. It includes a series of operations, some operations include replacing the input bits by specific outputs, these operations are called substitutions and other operations involve shuffling bits around, these operations are called permutations.

AES (Advanced Encryption Standard) performs all of its computations on bytes instead on bits. AES treats 128 bits of a plaintext block as 16 byte block. Number of rounds available in the AES is variable and it mainly depends on the length of the key that is being used. AES (Advanced Encryption Standard) uses 10 rounds if key is 128-bit, 12 rounds if key is192-bit and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is basically calculated from the original AES key.

The main purpose for choosing AES algorithm for encryption is its support for larger keys, and it's more secure than DES (Data Encryption Standard) algorithm, it's also faster in both software and hardware.

After encrypting all the file parts, combiner module stores the parts in respective servers. The advantage of storing it in multiple servers is even when the attacker gets hold of contents of one server which basically means that one server is compromised, attacker will only be in possession of a part of file which is in encrypted form. In the worst case scenario even if the attacker gets hold of all parts of file, attacker has no clue of how to combine all these parts since attacker don't know the contents of the file parts.

When user wishes to retrieve the file, combiner module collects all parts of file from different servers and decrypts all parts of file with corresponding server keys on which these parts were stored. Once the user retrieves the file, the user can decrypt the file with the private key with which it was encrypted after uploading the file.

4. CONCLUSIONS

Many organizations and businesses related to safe storage and security will be benefitted by this solution, since the problems related to security of files stored in cloud will be solved with this approach. It is very risky to put whole file in only one cloud server as this increases the possibility of attacks and attacker gets hold of entire file contents. So by implementing this methodology there is an increase in the security of files stored in cloud by storing in different servers and encrypting them. It uses multiple cloud storage concepts along with the concept of encryption to increase the security of contents in cloud, rather than storing entire file on one cloud system, it will split the file into number of chunks, hash them and encrypt them and store them in different cloud servers. This methodology allows the organizations to have an upper hand on their files with the two level encryption adopted here with an additional advantage of Data Integrity.

4. FUTURE ENHANCEMENTS

There are various encryption algorithms which impose greater security on the files which can be used in this specific use case, as encryption is made modular allowing the system to be improvised with more advanced encryption algorithms developed in the future. The process can be made Highly Available (HA) by backing up the contents of each of every part in different servers just to make sure that if one server fails the user must not lose the content that is stored on that particular server. Furthermore, better key management strategies can be adopted to manage the keys used for encryption.

ACKNOWLEDGEMENT

A lot of analysis and reading was done prior to the curation of the content of the given paper. This would definitely not be possible under the guidance of our mentors, Prof. Raghavendra Prasad, Prof. Smitha G R, who constantly guided and gave a direction in the due course of the given paper. We would also like to thank our Head of Department, Dr. B.M. Sagar, who gave us this opportunity to work on this paper.

REFERENCES

[1] MohammedA. 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.

[2] Tran Doan Thanh, Subaji Mohan, EunmiChoil, SangBum Kim, Pilsung Kim "A Taxonomy and Survey on Distributed File Systems," IEEE Fourth International

Conference on Networked Computing and Advanced Information Management, 2008.

[3] Satyanarayanan, M., "A Survey of Distributed FileSystems," Technical Report CMU- CS-89- 116, Departmentof Computer Science, CarnegieMellonUniversity, 1989.

[4] PavalBzoch, Jiri Safarik, "Security and reliability of distributed file systems," *6th* IEEE international con. on intelligent data acquisition and advanced computing systems, Sep 2011.

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

[6] Wang Liang-liang,ChenKe-fei,Mao Xian-ping,Wang Yong-tao —Efficient and Provably-Secure Certificateless Proxy Re-encryption Scheme for Secure Cloud Data Sharing‖ Journal of Shanghai Jiaotong University Volume 19, issue 4,2014 pp 398-405.

[7] Manoj V. Bramhe, Dr Milind V Sarode, Dr Meenakshi S Arya, "MultiCloud secure data Storage using Cryptography Techniques, International Journal of Research in Advent Technology, January 2019.

[8] Dr K Subramanian, F. Leo John- "Enhanced Security for Data Sharing in Multi Cloud Storage (SDSMC)", IJACSA,2012.

[9] Deepak Jain, Nidhi Singh – "Providing security using encryption and splitting technique over cloud storage", International Journal of Enginering Science and Research Technology, June 2018.

[10] Dan Dobre, Paolo Viotti, Marko Vukolic, " Hybris: Robust Hybrid Cloud Storage", ACM Transactions on Storage, Vol . 13, Issue 3, October 2017.

[11] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, Yafei Dai, " CHARM: A Costefficient multi cloud data hosting scheme with high availability," IEEE Transactions on Cloud Computing, Vol. 3, Issue 3, July-September 2015.

[12] Alysson Bessani Miguel Correia Bruno Quaresma Fernando Andre Paulo Sousa, " DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", ACM Transaction on Storage, Vol. 9,No. 4, Article 12. November 2013.

[13] Selvakumar G. JeevaRathanam M. R. Sumalatha ," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012.

[14] Prashant Kumar, Lokesh Kumar," Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 1, December 2013.

[15] J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D," Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm," in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010