Dynamic Data Slicing in Multi Cloud Storage using Cryptographic Technique

Dr.K.Subramanian[1]
[1] Assistant Professor, PG and Research Department of Computer Science, H.H The Rajah's College, Pudukkottai,
Emai-subjjcit@gmail.com

F. Leo John* [2]
[2]Research Scholar, P.G and Research Department of Computer Science, JJ. College of Arts & Science (Autonomous), Pudukottai
Emai-stleojohn@gmail.com

***Abstract*- In the modern era of computing, secure data sharing has become one of the challenges when considering the adoption of multi-cloud storage services. It has become one of the essential services in cloud computing. Many advantages of multi-cloud storage attracts the individuals and organization to move their data from remote to cloud servers. Recently many Multi-cloud storage services have been proposed but most of them focus on the single specific organization and file formats. In addition most providers use attribute based encryption which encrypts only particular database fields which reduces the trust of the many individuals and organizations. The biggest challenge that the present business world faces in multi-cloud storage is that there is no single standard architecture and procedure that can meet the requirements of the individuals and organizations. In order to address this challenge, this paper presents an effective architectural framework with a standard algorithm which would enable to enhance the secure data sharing through dynamic index based cryptographic data slicing. The proposed model is suitable for decision making process for the individuals and organizations in the adoption of multi-cloud storage service based on trust.**

Key words- Multi-cloud, Security, Data Sharing, Cryptographic data slicing

I. INTRODUCTION

Multi-cloud is the combination of public, private or managed clouds including managed services or service providers. Multi-Cloud data systems have the capacity to enhance data sharing and this aspect will be significantly of great help to data users. Most business organizations share most of their data with either their clients or suppliers and consider data sharing as a priority [1]. Through data sharing, higher productivity levels are reached. From the business point of view most cloud service provider offers only attribute based encryption. This type of encryption is based on few database fields such as account number, passwords etc. In [2] and [3] attribute based encryption is used to protect the patient's information in health care organization. In order to reduce the cost of cloud hosting cloud storage providers prefer attribute based encryption.

II RELATED WORK

Privacy and security for cloud storage are generally a wide area of research. Numerous academic interrogations have been conducted to identify the potential security issues about this subject. In [4] authors provide an architecture and a standard procedure for secure data sharing in clouds. But most of the security operations such as key management, user group management, and encryption and decryption process is maintained by third party provider. None of them approaches splits the file using the defined parts. Each part gets encrypted and stored in the multi-cloud.

meet the requirements needed by the individuals and organizations.

In [5], [6], [7] authors proposed the proxy re-encryption scheme using proxies to enhance the session key security in a single cloud storage. In [8] author describes architecture that uses cryptographic data splitting to store the data in the multi-cloud server. This method failed in uploading the video files. The proposed model is very similar to [8] because both approach tries to enhance the confidentiality to the customers. But in [8] suitable for small sized files and it takes higher computation in splitting the large files since the splitting is based on fixed size defined in the prototype.

III. PROPOSED SYSTEM MODEL

The typical proposed architectural framework model is shown below.

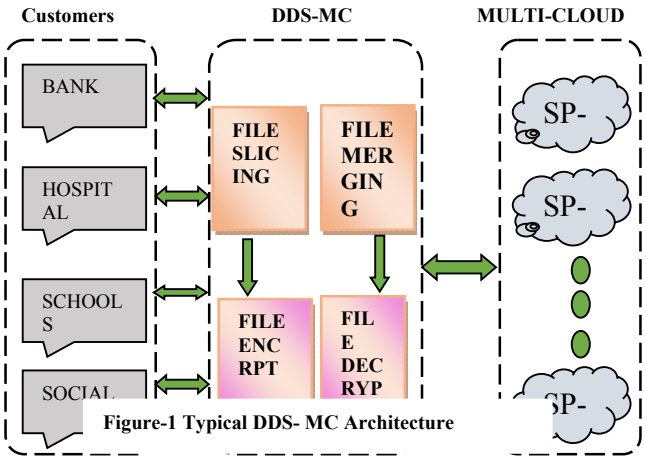

Figure-1 Typical DDS- MC Architecture

As shown in Fig. 1, the cloud customers make their requests to the proposed system called Dynamic Data Slicing in Multi-Cloud (DDS-MC). The DDS-MC system has different components having their responsibilities to find the required services from the appropriate service providers. The responsibilities of each component are given in detail in the following Section.

The Overview of Secure proposed framework components is shown in Figure-2. The proposed methodology guarantees that file slicing parts are defined by the data owner limited to the available storage locations. Data owner uploads the file through the proposed framework interface. The framework

978-1-5090-5573-9/16 $31.00 © 2016 IEEE
DOI 10.1109/WCCCT.2016.46

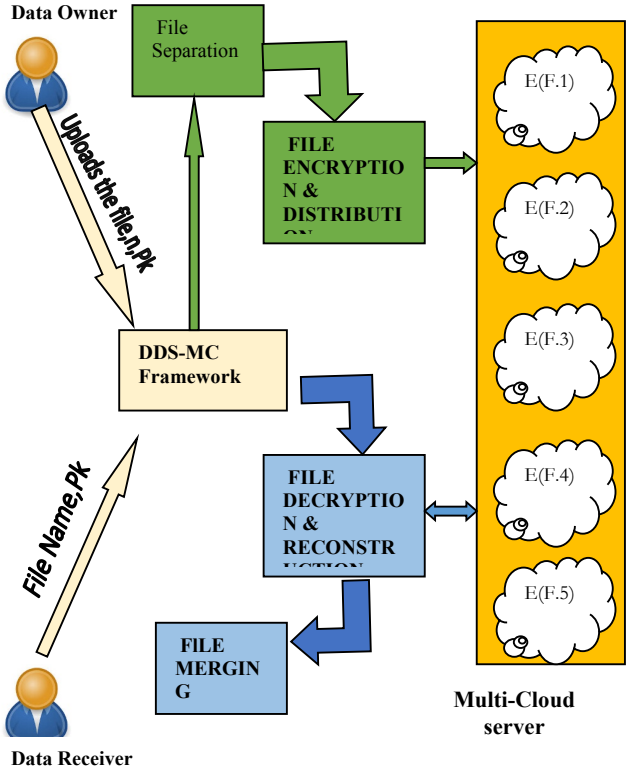

Figure-2 DDS-MC FRAMEWORK COMPONENTS

The receiver sends the decryption request to the owner. After the successful verification owner acknowledges the decryption request and send the necessary credentials for downloading the file. The receiver enters the credentials through the framework interface. The framework retrieve the file parts and each parts get decrypted and stored the receiver's machine.

The receiver or the service provider does not have any knowledge about the number of file parts stored in the multi-cloud server. This method also ensures the file cannot get access without the knowledge or permission of the owner.

In the above figure-2 the symbol F represents file name, n represents user defined number for file slices, and numerals(1,2,3) represents the indices of the sliced files

At its core the architecture consists of the following components and operations. Each component is associated with the framework.

Data Owner-A cloud user named data owner share or upload the file by using the framework interface in addition with private key and number of file parts to slice the file.

File Separation-The framework divides the file and stored in the local server.

File Encryption and Distribution-Each part of the sliced file gets encrypted by the framework and gets stored in the multi-cloud server.

Multi-cloud server-It consists of many storage servers. Encrypted file parts are stored securely.

Data Receiver-The receiver gets the necessary details from the data owner to download the file

File Reconstruction and Decryption-The receiver submit the file name and private key through the framework which in turn searches the file name in all the available storage locations and decrypts the matched file parts.

File Merging- The decrypted file parts are merged to give the whole information to the receiver.

Table-I Notation and Description Table

Acronym	Description Table
F	File
Fn	File Name
F1,f2,f3,f4,f5	File parts
Pk	private key
n	Number of file parts to be divided
E(f1),E(f2),E(f3)	Encrypted file parts

Algorithm-1 DDS-MC File slicing and encryption

```
Input File f, pk, n
Output E(f1),E(f2),E(f3)
Begin
Compute
For int i=0 to n
Split( f(i))
Encrypt(E(f(i))
Store E(f(i))
Next
End
```

Algorithm-2 DDS-MC File merging and decryption

```
Input fn, pk
Output f
Begin
 Search fn in multi-cloud
Compute
While(fn match)
n=n+1
end while
For int  i=0 to n
Retrieve E(f(i))
 Decrypt(E(f(i))
Merge( f(i))
Next
End
```

IV IMPLEMENTATION

The proposed methodology is used to provide the following services to the outsourced data

- Confidentiality and secure distribution of data sharing in multi-cloud
- Ability to support various file formats including video files
- Removal of centralized distribution of data
- Prevent colluding service provider attacks
- Dynamic file slicing options to data owner

a) Experimental Setup

To evaluate the performance of the proposed methodology the **DDS-MC** framework is implemented in Visual Studio 2010 C# using .Net framework4.0. . All the entities were operated on windows 7 professional 64 bit machine. The machine uses an Intel® Core (TM) 2 Duo CPU T6500 that runs 2.10 GHZ with 4GB of DDR3 RAM. This methodology uses at least five multiple private clouds for each files in experimental setup.

b) Results and Discussions

The Table-1 below shows the turnaround times for the encryption and decryption process based on the various file formats. The figure-2 shows the turnaround performance for the various file formats.

Table-1 shows the encryption and decryption time for the various file formats

S.No	File Type	File Size(MB)	Encryption Time (SECS)	Decryption Time (SECS)
1	proj.docx	26.3	01	01
2	Proj1.pdf	36.4	02	02
3	Bank1.xpt	79.3	04	05
4	Bank2.xpt	91.3	05	06
5	utube.avi	108	06	07

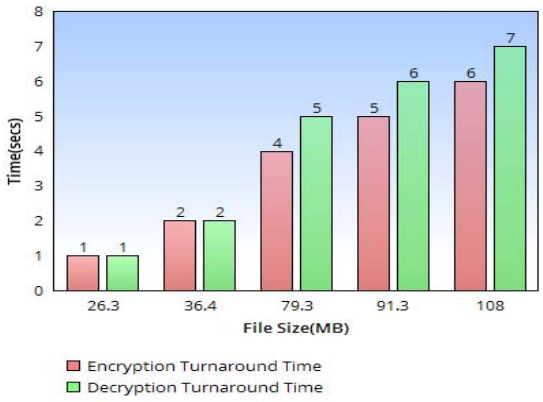

Figure-3 Encryption and Decryption Turnaround Performance for Various File Formats

c) Performance Evaluation

The results obtained from our technique indicate that all processing steps of our architecture can be accomplished with good performance. Figure-3 shows the performance of the proposed technique. However, it's more important data owner's waiting time should be minimal for larger file size (500 MB).Since the current implementation performs all operations in memory CPU processing power and memory resources are also concern in performing this technique. It is therefore favorable to operate the proposed technique in firm Multi Cloud Server Environment.

V. CONCLUSIONS AND FUTURE ENHANCEMENT

The proposed technique is well suited for individual as well as organizational aspects. This approach also overcomes the challenges discussed in related works such as ability to upload various file formats, colluding service provider attacks to retrieve meaningful information, removal of centralized distribution of storage and provide better decision making process for the individuals and other organizations in adopting the best multi-cloud storage services. The results from our implementation indicates the practical feasibility and good performance for secure data sharing in Multi Cloud Storage.

Again, throughout the research work, there has been the assumption that no cloud storage service provider may have malicious intentions of the stored data. In future additional features such as nonrepudiation, dynamic symmetric encryption can be combined along with this approach to enhance the trust of the customers.

REFERENCES

[1] Balasaraswathi,V. R., & Manikandan, S. (2014). Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach. In *Advanced Communication, Control and Computing Technologies (ICACCCT), 2014 International Conference on* (pp. 1190-1194). IEEE.

[2] Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150.

[3] Tatiana Ermakova, Benjamin Fabian Secret Sharing for Health Data in Multi-provider Clouds Business *Informatics (CBI), 2013 IEEE 15th Conference (2013)* pp 93-100.

[4] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan Athanasios V. Vasilakos (2014). *SeDaSC: Secure Data Sharing in Clouds,* Systems Journal, IEEE pp 1-10.

[5] WANG Liang-Liang, CHEN Ke-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 (2014)* Volume 19, issue4, pp 398-405.

[6] Seo, S. H., Nabeel, M., Ding, X., & Bertino, E. (2013, September). An efficient certificateless encryption for secure data sharing in public clouds. *Knowledge and Data Engineering, IEEE Transactions on*, *26* (9), 2107-2119.

[7].Khan, A. N., Kiah, M. M., Madani, S. A., Ali, M., & Shamshirband, S. (2014, May). Incremental proxy re-encryption scheme for mobile cloud computing environment. *The Journal of Supercomputing*, *68* (2), 624-651.

[8] Peng Xul, Xiaqi LiU, Zhenguo Sheng, Xuan Shan', Kai Shuang SSDS-MC: Slice-based Secure Data Storage in MultiCloud Environment *11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (QSHINE 2015) pp 304-309.

[9] Yuuki Kajiura, Shohei Ueno, Atsushi Kanai, Shigeaki Tanimoto, Hiroyuki Sato An Approach to Selecting Cloud Services for Data Storage in Heterogeneous-Multicloud Environment with High Availability and Confidentiality *Autonomous Decentralized Systems (ISADS 2015) IEEE Twelfth International Symposium* (pp 205 – 210).

[10] Hendrik Graupner, Kennedy Torkura, Philipp Berger, Christoph Meinel Secure Access Control For Multi-Cloud Resources *Local Computer Networks Conference Workshops (LCN Workshops), 2015* pp 722-729.

[11] Hazila Hasan, Sultan Abdul Halim Muadzam Shah Secured Data Partitioning in Multi Cloud Environment *Information And Communication Technologies (WICT), 2014* pp146-151.

[12] Xu, L., Wu, X., & Zhang, X. (2012, May). CL-PRE: A certificate less proxy re-encryption scheme for secure data sharing with public cloud. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (pp. 87-88). ACM