iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3173

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Improved Security for Data Sharing In Multi Cloud Storage (SDSMC)

Mayavathi. M[1], Dr. S. Chandrasekaran[2]
[1]*PG Student and* [2]*Assistant Professor, Department of Computer Science and Engineering, P.S.V. College of Engineering & Technology, Krishnagiri*

Abstract: ***Multiple Cloud storage has become one of the essential services of cloud computing. This Multi-Cloud storage models allow users to store sliced encrypted data in various cloud drives. Thus, it provides support for various cloud storage services using the single interface rather than using single cloud storage services. Cloud security goal primarily focuses on issues that relate to information privacy and security aspects of cloud computing. This latest data storage service and data moderation prototype focus on malicious insider's access on stored data, protection from malicious files, removal of centralized distribution of data storage and removal of outdated files or downloaded files frequently. Data owner does not necessarily need to worry about the future of the data stored in the Multi-Cloud server may be extracted or depraved. The other is ingress control of data. The proposed method ensures the file or data cannot get access without the knowledge or permission of the owner. This technique will offer a secure environment whereby the data owner can store and retrieve data from Multi-Cloud Environment without file merging conflicts and prevents insider attacks to obtain meaningful information. The experimental results indicate that the suggested model is suitable for decision making process for the data owners in the better adoption of multi-cloud storage service for sharing their information securely.***

I. INTRODUCTION

Multi-Cloud is the utilization of various computing services in a single heterogeneous architecture. Multi- Cloud Storage means the utilization of various cloud storage services using a single web interface rather than the defaults provided by the cloud storage vendors in a single heterogeneous architecture.

Multi-Cloud data systems have the capacity to enhance data sharing and this aspect will be significantly of great help to data users. It enables data owners to share their data in the cloud. In any cloud computing model, security is regarded as the most crucial aspect due to the sensitivity and delicacy of the user's information or data stored in a cloud. Presently, every Organization is pushing its IT department to scale up their data sharing systems. Most cloud services are not free and possess different sizes. For instance, Single Cloud Storage falls among the services with storage limitation which makes it disadvantageous in comparison to multi-cloud storage.

The main advantage of using multi cloud storage is performance and higher security for data sharing. In the single cloud storage data remains on the centralized storage which can be easily accessed by the malicious insiders. Companies should start considering working with more than one cloud provider at a time - for cost savings, performance, disaster recovery and other reasons. Most business organizations share most of their data with either their clients or suppliers and consider data sharing as a priority.

II. RELATED WORKS

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. It is important to note that sharing files over cloud platform possess numerous vulnerabilities that can lead to unauthorized access.

The attackers of cloud have varied intensions or goals which leads to the poor image of the cloud providers once the goal is achieved.

The main drawback in this approaches are group sharing requires huge computation and long waiting time, since file indexing is not used ambiguous information results in file retrieval process. Since the CP-ABE is provided by third party malicious insider may have easy access to the data. File size more than 50 MBs increase the customer's waiting time. The experiments are performed using a highly configured machine hence it is cost consuming in real time. Malicious files are also easily uploaded by the third party authority or role based managers to corrupt the entire scheme.

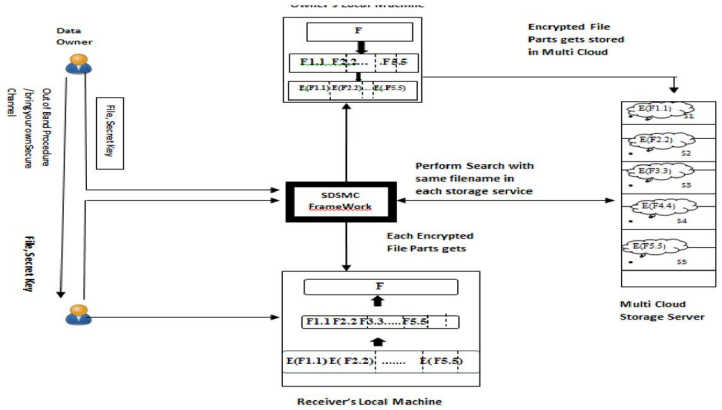


Fig.2.1 Security for cloud storage

III. PROPOSED SYSTEM MODEL

The Overview of Secure Data Sharing Multi Cloud (SDSMC) is shown in Figure-1 and the details are provided in Section 4. The proposed methodology guarantees the file slicing with index based parts gets encrypted and stored on the Multi-Cloud. This method ensures the file cannot get access without the knowledge or permission of the owner. Data owner uploads the file through the proposed framework interface. The framework uploads the file in the local machine. The framework splits the file with its indexes assigned and encrypts each part of the file using the secret or private key provided by the owner. Each part of the encrypted file gets stored in the owner's machine and then transferred to the multi-cloud server. The receiver sends the decryption request to the owner or the owner can share the required credentials through Bring Your Own Secure Channel (BYOC) or out of band procedure. The receiver enters the credentials through the framework interface. The framework retrieve the file parts and each parts get decrypted, merged and stored the receiver's machine. The major contributions, as described in this report are as follows. The unique feature of this system is to protect the data access from malicious insiders and to protect the datacenters information from malicious files .In addition it also has provision the index based cryptographic data slicing in Multi-Cloud storage services to reduce the file merging conflicts and on demand cost for the customers.

A. SDSMC Framework

The Secure Data Sharing in Multi Cloud (SDSMC) framework is a web application and it has been described with the overall system flow and various procedures. File uploading, index based file slicing, file encryption, file distribution, file decryption, file retrieval and merging of files, file deletion and Unicode conversion are the automated process performed by the SDSMC framework when using the interface while uploading or downloading a file.

1) *File Uploading:* Data owner browse the file from local machine and uploads the file using SDSMC framework interface. This framework uses client resources to upload the file. It means file gets uploaded in the local machine.
2) *Indexed Based File Slicing:* This is the process of dividing the uploaded file into two or more parts with respective indices. In this process file slicing is based on the number of storage providers available in the multi-cloud server. At least five storage providers must take part in data sharing and data retrieval process in the proposed approach. This process happens in the owner's local machine.
3) *File Encryption:* This is the process of converting a readable file in to unreadable format. This framework encrypts all the index based sliced files using Advanced Encryption Standard (AES) algorithm. Although many existing approaches uses AES it has two draw backs. First it is a weak cipher and the second 128 and 256 bits key make the turnaround time higher which affects the turnaround time process and makes client to wait for a longer time. To overcome the above said limitations slicing is used to make it strong cipher and user defined secret key is used to reduce the turnaround time.
4) *File Distribution:* The process of sending the encrypted files along with their indices to different cloud storage providers available in the multi cloud server.
5) *File Retrieval:* It is the reversal process of file distribution and file slicing. It is also known as file reconstruction. In this framework the retrieval process starts with submitting the filename without extension. This framework searches the specified filename in each and every cloud storage in multi-cloud server.
6) *File Decryption:* Every filename from the multi-cloud server which is associated with specific filename submitted gets decrypted sequentially and stored in the local receiver's machine.

7) *File Merging:* This is the process of joining the files with respective indices and gets stored in the receiver's local machine.
8) *File Deletion:* This framework performs the automatic removal of files from multi-cloud server and file merging parts in the receiver's machine after the completion of retrieval process.

The idea is about using multiple private clouds simultaneously to deter the risk of disclosure, process tampering and above all, data manipulation in a malicious manner.

IV. ARCHITECTURE OVERVIEW

Figure-1 describes a high level, a standard architecture for a multi-cloud storage service. In the Figure-1 F1.1, F2.2,.. F5.5 denotes the slice file parts name with its index. Similarly E(F1.1),E(F2.2)…E(F5.5) denotes the encrypted sliced parts with its indexing. S1, S2, S3, S4 and S5 are various storage service providers At its core the architecture consists of the following components:

1) *Data Owner:* The owner uploads the file with private or secret key. Data Owner acknowledges the request sent by the receiver and sent the details required for the decryption process through the out of band procedure or Bring your own secure channel (BYOSC). In addition the data owner maintains the authorized user's list and keys. Data owner performs the third party duties.
2) *Key Management:* There are three options to manage the keys in cloud storage. They are provider's data center, third party server and customer premises. To enhance flexibility and enable sharing of a file to another spacer, it is beneficial to induce the private key at the owner's premise in this approach, as in amazon S3 storage has an enabling option to manage the owner keys.
3) *Multi Cloud Server:* It consists of various trusted storage service providers like Cloud A, Cloud B, Cloud C. It stores the encrypted parts of the sliced file from the SDSMC framework to the specific storage service. In this approach minimum five trusted storage service providers are used.
4) *Data Receiver:* The receiver will act as a secondary user or sub user. Once the required details are obtained from the owner file can be downloaded.

a) *Algorithm -1* explains the application data or file is sliced and transmitted to distinct clouds based on the number of storage services. Files are the most used forms of data storage. The file is uploaded by the user to the Multi Cloud server. The uploaded file gets sliced into five parts with respective indices had been assigned and each part is encrypted using AES encryption algorithm. Five encrypted files are stored in the Multi Cloud Server with respective storage services
b) *Algorithm -2* describes the reverse process of encryption in which authorized receiver using the framework interface passes the file name and secret key obtained from the data owner. The framework start searching the filename associated in the multi-cloud server and then decrypts the file slices sequentially based on the indices and store the decrypted parts in the receiver's locations and finally merges the file based on indices. The merged file is downloaded at the receivers end. After the retrieval process decrypted and encrypted parts of the files are removed from the multi-cloud server and receiver's machine.

V. IMPLEMENTATION

The Secure Data Sharing in Multi Cloud (SDSMC) methodology is proposed to provide following benefits to the outsourced data:

1) Confidentiality and secure distributed data sharing in clouds
2) Provide protection from colluding service provider attacks
3) Removal of centralized distribution of file storage.
4) Automation of all the process such as file uploading, file slicing and indexing, encryption, decryption and merging.
5) The file is stored on minimum of five storage service providers
6) Self-protection of malicious files
7) Insider attackers are not able to retrieve meaningful information.
8) Removing of file merging conflicts in the retrieval process

A. *Architectural Setup*

The proposed methodology involves the creation of five private cloud storage services. There is no federated system is available to evaluate performance of the technique. The proposed Secure Data Sharing in Multi Cloud (SDSMC) methodology has been implemented in Visual Studio 2010 Asp.Net with C#. It consists of two entities Multi Cloud Storage Server and Users. The functionality or procedure required by the user is implemented as a client application that connects with Multi Cloud Server to receive the services. The SDSMC web application splits the uploaded file into n pieces based on number of storage services. Each file part has been assigned with indices and encrypted using Advanced Encryption Standard (AES) algorithm to be stored in the respective storage services.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

B. Numerical Security Analysis

The high level assessment of this multi-cloud approach is performed on the security features such as privacy, insider attacks, confidentiality, secret keys, and data integrity. Table-2 shows the percentage of security obtained in the proposed SDSMC approach. Three models Cipher Text policy Attribute Based Encryption (CP-ABE), Secure Data Sharing in Clouds (SedaSC) and proposed Secure Data Sharing in Multi-Cloud (SDSMC) are allowed in the private clouds for the specific period of time. The results obtained from our technique indicate that all processing steps of our architecture can be accomplished with good performance. 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.

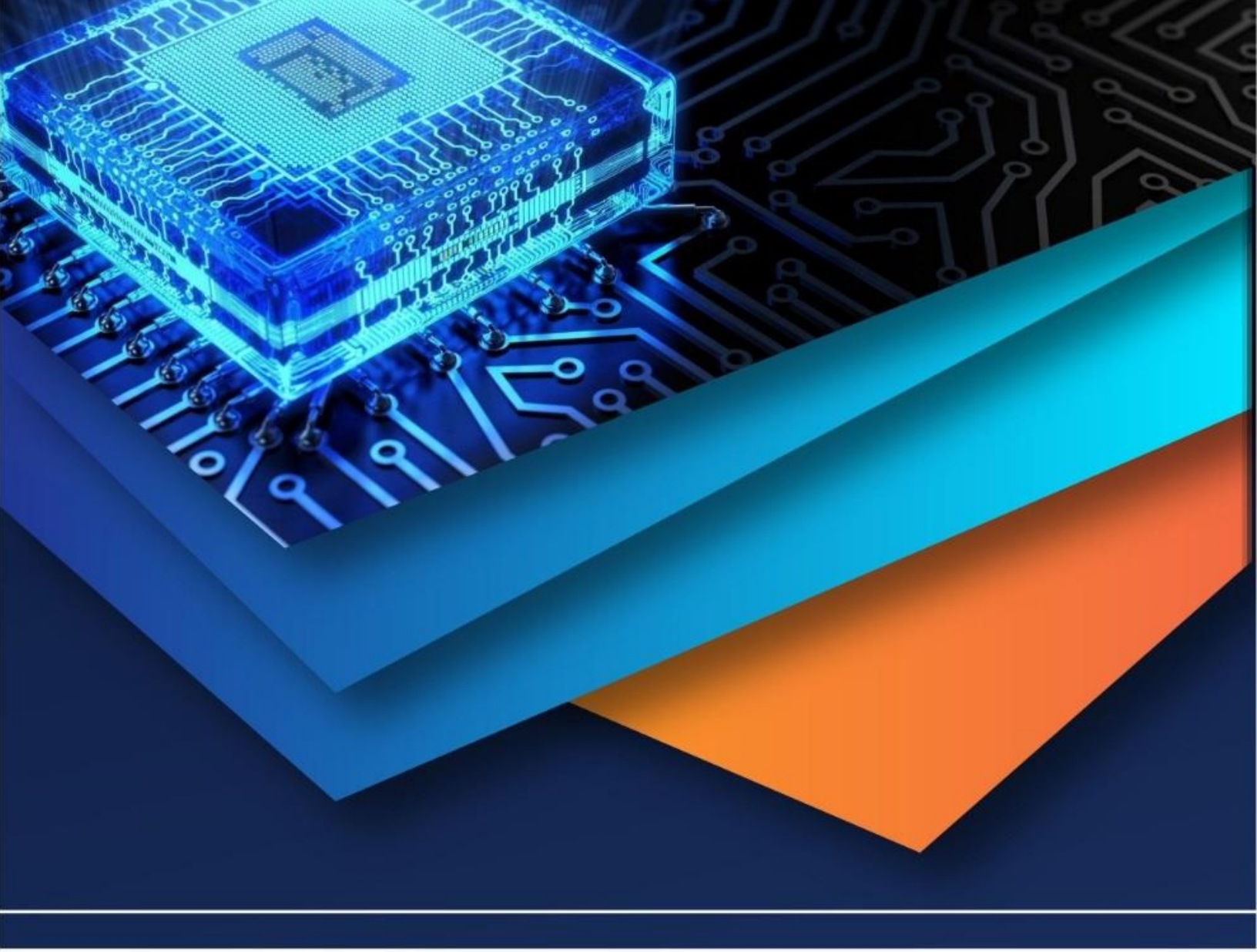
Fig. 4.1 Encryption & Decryption

VI. FUTURE WORK

Although the proposed model ensures the protection of data sharing from malicious insiders and files there is a possibility of leakage of key without the owner's knowledge when the framework interface gets accessed from the public networks. When the data owner tries to upload the more files key management becomes cumbersome. To rectify above problems system a public key hybrid crypto system is needed. To enhance the trust of the customers file slicing parts can be defined by the owner itself is the other future directions of our proposed model.

VII. CONCLUSION

The proposed methodology is a Multi Cloud Storage security scheme for organizational as well as non-organizational aspects. Since the various data sets have been used to operate on the SDSMC model and reaches the higher security when compared with other models. The proposed architecture reduces the malicious insider threats and the proposed procedure ensures the providers resource protection from the malicious files. The SDSMC supports all type of files including video files can be encrypted based on the index based cryptographic technique. In the retrieval of the files a standard procedure is used which reduces on demand cost and the conflicts in the merging process. The experimental results justify the efficiency of the proposed algorithm. The numerical results justify the data sharing security of the proposed model.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY