Secure Multi Cloud Storage Approach for Personal E-files

Amit Gadekar[1], Mahalaxmi Bhandari[2], Manorama Ahire[3], Albaana Mirza[4], Suraj Yadav[5]
Department of Computer Engineering[1, 2, 3, 4, 5], Affiliation name[1, 2, 3, 4]
Email: amit.gadekar@sitrc.org[1], bandarimalaxmi@gmail.com[2]

Abstract- Cloud computing provides a numerous ways for the users of the large amount of virtual storage. Now a days cloud computing is used in many areas like industry, military, colleges, etc. to storing huge amount of data. There are many files and documents which are very important for some purpose. We can retrieve data from cloud on the request of the users. These documents are to be stored and secured very efficiently. The security of the documents is mandatory because as no third party can be viewed that documents. To provide the solution to the documents there are n number of solutions. Data confidentiality is providing the data securely and safely in the clouds and while sharing the files between the users, the file should not be viewed by any third party agent. The user has to simply create their own account in the application. For the storage of the files in various formats, different cloud storage is used. The security of the documents is necessary to maintain each and every file in the cloud safely and properly. The algorithms of cryptography are the most widely used algorithms now for the encryption of files. Here the file is divided into blocks and these blocks are encrypted with same or different algorithm. These files are then stored in different storage of public and private clouds. The user can request a document to a public or specific other user. Other users will get the request and they can either accept or deny it. We are going to use QR code for every single file. Without QR code no one can read the file, no one can download the file, etc.

Index Terms- Cloud computing; Distributed data storage; Cryptography; Encryption; Decryption; etc.

1. INTRODUCTION

Cloud computing is a delivery of computing services over the internet. Cloud computing allows accessing information as well as resources from anywhere from where the network connection is available. But there is a draw-back that if it has no internet connection than the services are not available and also it can’t provide integrity for client’s data. Many organizations use the cloud computing technology due to its rapid increasing towards the industries. It provides the benefits in terms of very low cost and easily accessibility of the data. As the user stores most sensitive information in he cloud, the cloud vendor should ensure the security of the cloud storage which is the major factor in the loud computing environment. But these providers may be untrusted. Dealing with the “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “inter-clouds” or “cloud-of-clouds” has emerged recently. The basic idea is to secure the files/documents after storing in the multiple clouds. The third party agents also known as hackers, can view or attack the file and can use for various malicious activities. For this purpose we divide the files into blocks and each block is encrypted by using same or different algorithms. Some delimiters are added into file to recognize file blocks. A user can store a document as public or send to a specific user. We are providing a QR code for each file. Using QR code only, the user can view the document or download it.

2. METHODOLOGY

Module: In the first section, we will be described our cloud storage module and system module. We will describe our problem statement. We are going to note that the work on cloud service provider and the service provider to interchangeable, in that we are denied the cloud storage are the interchangeable.

2.1. *Secured Multi Cloud Storage*

Storage In that multi cloud storage are used for the cloud data storage into multiple clouds and also provide the multi service providers. In each cloud storage represents a different multiple services providers. In that actual cloud server is implemented by different cloud service providers. In multiple cloud storage the obvious objectives is that minimize the cost of storage of the data part over service providers.

2.1.1. *Distributed Cloud Storage*

To ensure the availability and reliability of the data, distributed storage is considered within the cloud provider. A distributed cloud storage uses data-center topology, a topology in which the cloud storage provider has numerous data-centers that can be spread over a large geographical area and in which the user stores and retrieves data from the data-center closest to it [2]. A distributed cloud-storage consists of a peer-to-peer distributed cloud storage solution. It protects your files, both on the nodes and in transmission, by using cryptography to encrypt files.

2.1.2. Multi Cloud strategy

To minimize the risk of service availability failure, loss of the data and loss of privacy, multi cloud strategy is used. Multi-cloud strategy is the use of two or more clouds. The usage of multiple clouds may reduce the risk for application and data in a public cloud and private cloud. The standard obstacles for adoption of cloud are such as security, reliability, cost and loss of control remain. Therefore by deploying multi-cloud environments, many organizations can gain more flexibility with the ability to determine what workloads to run where and more control over the services they use [3].

2.2. *Encryption and Decryption*

2.2.1. File level encryption and decryption

File level encryption and decryption File level encryption is also called as file-system level encryption which is used to encrypt the files/folders and is a form of disk encryption. The advantages of file level cryptography is access control is enforced through the use of public key cryptography, flexible file based key management, cryptographic keys are only held in memory while the file that is decrypted by them is held open. In the file level cryptography, the whole file is encrypted along with the structural details, the metadata of the file, the file ownership details, creation details, etc.

2.2.2. Block level encryption and decryption

In the block level cryptography, the file is rather divided into blocks so that we'll apply the encryption and decryption of the file for the blocks. These blocks are encrypted and later distributed to different cloud storage and stored in the multiple clouds. That is whenever the hacker hacks the cloud storage, even though he/she can only get a block of the document and cannot hack the whole document and can become the advantage for the application.

2.3. *Algorithms*

This project consists of two algorithms used in it i.e. Triple AES algorithm and Base 64 encoding algorithm.

2.*3.1. Triple AES algorithm*

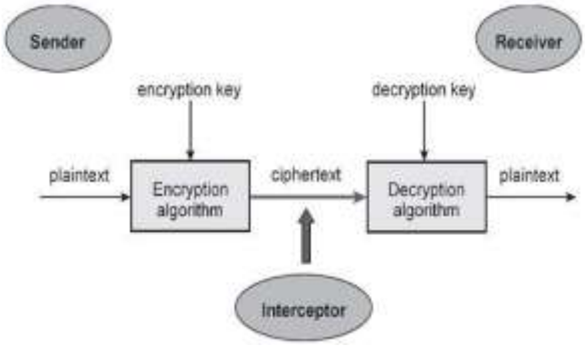

Fig. 1. Model of Conventional Cryptosystem

Figure 1 shows the model for conventional cryptosystem. Two cryptographers who belongs to Belgium developed the cipher based Advanced Encryption Standard. Rijndael is a family of ciphers having various block and key and these all are different from each other. The size of the block is 128 bits and the various lengths of the key are of 128, 192 and 256 bits. AES functions on a 4×4 column-major order matrix of bytes termed the state. For the conversion of plaintext into the cipher text, it requires many repetitions of transformation rounds and this is specified by size of key used in AES cipher:
For 128 bit keys 10 cycles of repetition are required.
For 192 bit keys 12 cycles of repetition are required.
For 256 bit keys 14 cycles of repetition are required.

AES algorithm is that its implementation can be done both in software and hardware while DES can only be implemented in hardware^5.

2.3.2. Base 64 Encoding algorithm

Base64 is not an encryption method, but it is the standard encoding. Base64 is a block cipher algorithm which is operated on a bit, but the Base64 mode is much easier in its operation than the other algorithms. Base64 is a general term for some similar encrypting system that encrypts binary data and converts it into a representation of the base 64. This project divides the file/document in the four parts/blocks by which the size of the file is divided by 4 and each block of the file is converted into the string format which cannot be viewed or understand by the third party agent and can be confidentially and securely transferred between the two users.

3. DOCUMENT CLASSIFICATION

The project classifies the saved documents into various sections such as educational documents, home appliance documents, bank services related documents and other documents. These documents are classified so that the user whoever uses the application can properly understand where the documents should be stored and also these documents/files can be classified as important and not important. The important file are given more security using two different algorithms. The non-important file are given less security and all the users can be able to see the non-important files.

4. PROPOSED WORK

The main focus is on the problems which are related to the security of data of the cloud computing. The file is divided into several blocks and gets encrypted and stored in multiple clouds. The files are categorized into two type's important files and non-important files. The important files cannot be seen by the other viewer. As we know that the encrypted files contain the encryption key along with it and only using that encryption key, we can access the document or else the file cannot be visible for us. Here this project uses the QR code as the encryption key for accessing the file.

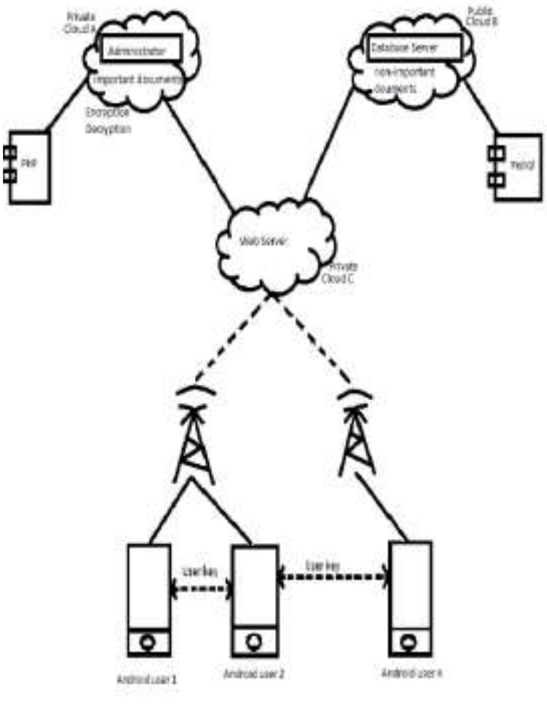

Fig. 2. Basic Architecture

Here, the user request for the file, the owner of the file receives the request and sends the file along with the QR code, if and only if the QR code gets same, then only the requested user can access the file, or else he/she does have access to the file.
The architecture of the proposed system is as shown above.

5. EQUATIONS

S= {U, I, O, D, P}
Where,
U = Set of users

$$U = \sum_{i=1}^{n} Ui = \{u1, u2, u3, \dots\dots\dots, un\}$$

Where n>0

I = Set of Inputs

$$I = \sum_{i=1}^{n} Ii = \{I1, I2, I3, \dots\dots\dots, In\}$$

Where n>0
= ex. Login details, personal information, signals, etc.

O = Set of Outputs

$$O = \sum_{i=1}^{n} Oi = \{o1, o2, o3, \dots\dots\dots, on\}$$

Where n>0
= ex. Login access/deny, lock open/close, camera on/off etc.

D = Set of Devices

$$D = \sum_{i=1}^{n} Di = \{D1, D2, D3, \dots\dots\dots, Dn\}$$

Where n>0
= ex. Android device, camera, etc.

D = Set of Processes

$$P = \sum_{i=1}^{n} Pi = \{P1. P2. P3. \dots\dots\dots. Pn\}$$

Where n>0
= ex. Authenticate, signal processing, sms sending etc.

Acknowledgments

We would like to take this opportunity to thank our internal guide Prof. Mr. Amit. R. Gadekar for guiding us throughout the project all we needed. We are really grateful for his continuing support and valuable feedback and for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

We are also grateful to Prof. Amol D. Potgantwar, Head of Computer Engineering Department, for his indispensable support, suggestions.

Results

The application can be used for various purposes for sending the files which are stored and protected securely on the multiple cloud servers. This app can be used in Government sector, Private sector, Defense sector, etc. There is a selection of documents in the app that the user can select the important or non-important document and then can upload the document. The document is directly switched to the server i.e. if important document then, the document is directly encrypted using Triple AES algorithm and divided into blocks using Base 64 encoding algorithm and the blocks are stored in different private clouds of important documents only. And if the document stored is non-important then the document is stored on the public cloud storage directly which stores non-important documents. Whenever the requested user prints the documents, the user has to put the reason for printing the document and only he/she can print. This also maintains the log file that shows how many prints took by which user and for what purpose.

REFERENCES

[1] Bharat, K.; Broder, A. (1998): A technique for measuring the relative size and overlap of public Web search engines. Computer Networks, **30**(1–7), pp. 107–117.
[2] Maurice Bolhuis: A Comparison between Centralized and Distributed Cloud Storage Data Centered Topologies, rp (1-8).
[3] M Sulochana; Ojaswani Dubey. (2015): Preserving Data Confidentiality using Multi-Cloud Architecture, 50(1-6), pp. 357-362.
[4] Isnar Sumartono; Andysah Putera Utama Siahaan; Arpan (2016): Base64 Character Encoding and Decoding Modeling, pp. 2455-1457.
[5] Gagandeep Singh Walia.; Narinder Pal Singh.; Hunny Pahuja.; Amandeep Singh.(2016): Implementation and Analysis of Triple AES in VHDL, 9(47), pp.0974-5645.