SECURED M-CLOUD STORAGE SYSTEM

Shailesh Kamble[1], Pooja Kumbhojkar[2], Shilpa Gulgonda[3], Tushar Waghmare[4], Prof. Revati Wahul[5]
Computer department MESCOE Pune
Email: Shaileshkamble7777@gmail.com[1], poojakumbhojkar777@gmail.com[2],
shilpaapatil12@gmail.com[3],twaghmare72@gmail.com[4],rmwahul@mescoepune.org[5]

Abstract

Cloud computing is a technology that uses internet and central remote servers to maintain data and application. In cloud computing storage providers are responsible for keeping data available and accessible. For storage of data relying upon a solo service provider is not very promising. Security is important factor related to the cloud computing. Also the political influence might become an issue with the availability of service. In addition, providing better privacy as well as ensure data availability, can be achieved by dividing the user's data block into data pieces and distributing them among the available SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block. Data is divided into number of data units and stored on different cloud servers, it will increase data availability and data security. It also provides cost effective storage to the customers, so that they can choose cloud service provider according to their available budgets.

Index Terms: cost-effective, cloud computing, cloud security, cloud service provider

I. INTRODUCTION

The end of this decade is marked by a paradigm shift of the industrial information technology towards a subscription based or pay-per-use service business model known as cloud computing. This paradigm provides users with a long list of advantages, such as provision computing capabilities, broad, heterogeneous network access; resource pooling and rapid elasticity with measured services. Huge amounts of data being retrieved from geographically distributed data sources, and non-localized data-handling requirements, create such a change in technological as well as business model. One of the prominent services offered in cloud computing is the cloud data storage, in which, subscribers do not have to store their data on their own servers, where instead their data will be stored on the cloud service provider's servers.

II. MODEL

A. Problem statement

To develop an application over cloud storage using multiple cloud to store data and retrieve securely where given p number of cloud service providers (SPi: 1,2…p), each Service provider associated with a QoS factor (QoSi(0,1)) along with the cost of storing data units (Ci), it seeks a distribution of customer data pieces among the available service providers in such a way that, at least q number of service providers must take part in data retrieval, while minimizing the total cost of storing the data on service provider as well as maximizing the quality of service provided by the Service providers.

B. Overview

Cloud computing uses central remote servers to store data on it and provide efficient access to users data. Fig. 1 shows overview of cloud computing.

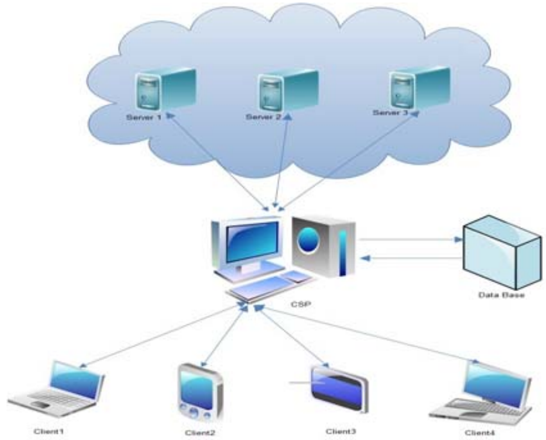

Fig. 1 Overview of cloud computing

We consider the cloud storage system in cloud computing that happens between Cloud User's (CU) and Cloud Service Providers (SP).Given P number of cloud service provider, Each service provider is having its own Quality of Service (QoS) and Cost for storing data. In this paper, user can analyse different Cloud Service Providers according to their cost and QoS as per their own requirement to store data. User can use multiple cloud vendors to store data independently. User can split data and store on different Vendors according to his available budget.

C. Overview of Functional Requirements

i. Administrators:
Understand clients' requirements for respective applications. As well as secure the database from illegal use.

ii. Developers/Employees:
It can retrieve the files related to application development.

iii. Client
Submission of complaints & requirements as well as it can retrieve the progress report of application.

D. Threat model

1. CSP Failure

When data is stored on single cloud service provider there are chances of single point of failure. When customer C1 stores his data on CSP1 and if server at cloud service provider gets failed then customer may loss his data. This is why customer can not depend upon single cloud service provider. To avoid such issue one solution is customers data will be stored on multiple cloud service providers.

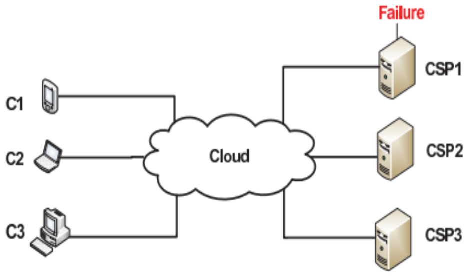

Fig. 1 CSP Failure

2. Colluding cloud service providers

Second threat is colluding service providers. In which cloud service provider might collude together to reconstruct data. As data is stored on multiple cloud service providers, user can not access the whole data until he has access to both the cloud service providers. So for successful retrieval of the data cloud service provider might collude together and reconstruct customers data.

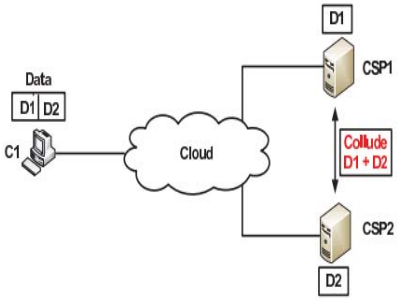

Fig. 3 colluding cloud service providers

III. ALGORITHM

An algorithm is an effective method that can be expressed within a finite amount of space and time and in a well-defined formal language for calculating a function. Starting from an initial state and initial input , instructions describe a computation that, when executed, proceeds through a finite number of well-defined successive states, eventually producing output and terminating at a final ending state known as algorithms.

A. Introduction to AES Algorithm

The Advanced Encryption Standard (AES) was announced by the National Institute of Standards and Technology(NIST) in November 2001. It is the successor of Data Encryption Standard (DES) which cannot be considered as safe any longer, because of its short key with a length of only 56 bits. There are three versions of AES. All of them have a block length of 128 bits, whereas the key length is allowed to be 128,192, or 256 bits. Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

B. Basic Concepts

The AES algorithm consists of ten rounds of encryption, as can be seen in figure 2. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes transformation using the corresponding cipher key to ensure the security of the encryption.

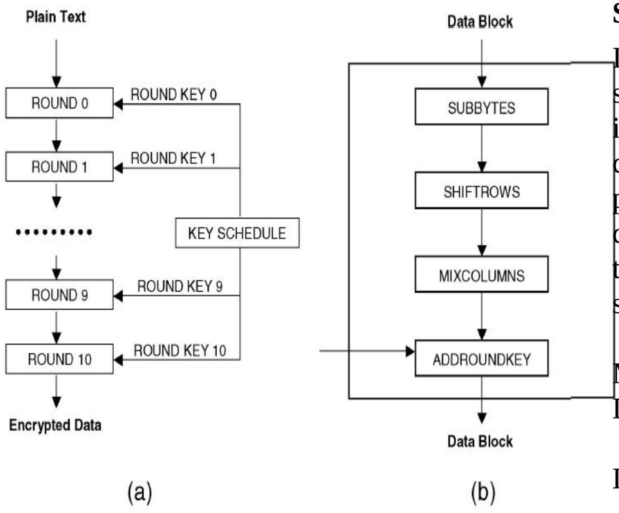

Fig. 4 Example of AES Algorithm

After an initial round, during which the first round key is XORed to the plain text (Addroundkey Operation), nine equally structured rounds follow. The 10th round is similar to rounds one to nine, but the Mix columns step is omitted.

TABLE I
FILE UPLOAD

C. Encryption:

Each round consists of the following four steps:

i. Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii. Shift Rows: In the encryption, the transformation is called Shift Rows.

iii. Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv. Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix, the operation in Add Round Key is matrix addition.

D. Decryption:

Each round consists of the following operations:

i. Inverse Substitute bytes

ii. Inverse Shift rows

iii. Add round key

IV. SECURED M-CLOUD STORAGE SYSTEM

In this paper, to mitigate the threats facing cloud storage, we extended the cloud data storage to include multiple service providers, where each cloud storage represents a different service provider. In this secured M-cloud storage system customers data is divided into different parts and these parts are stored on different multiple cloud service providers.

Module 1: User Validation & Upload File To Database

Let S1 be a set of parameters for Selecting File

S1= {File_Size ,File_Upload}

Uploading File data rate:- R=((N-NP) S/L)/N=S/L

Where ,

R is Binary data rate,

N is Size of file,

NP is size of data which carries the parameters, S is Small positive integer and L is size of binary data in file data.

Where,

File_Size = Actual size of file

File_Type = Type of File

Condition/Parameter	Operation/Function
If File_Type==Allowed	f1:Proceed()
Else..	Discard Operation

If image type is valid then proceed Else discard operation

Module 2: Self destruction Module

Lets S2 be a set of data

S2={ key }

Where,

key = Actual key of Data

TABLE 2
SELF DESTRUCTION MODULE

Condition/Parameters	Operation/Function
If(key is valid)	F2:Proceed()
Else	Data self deleted

If key is valid and user is legal then only proceed Else data deleted .

Module 3: Download File

Let S3 be the set of parameters to access Files & download file

S3: { Encrypted Text, File)

Where,

Encrypted_Image = It select an text file and encrypted in image with the authentication of user.

TABLE 3
DOWNLOAD FILE MODULE

Condition/Parameter	Operation/Function
If Encrypted_Key== valid	F3:Proceed()
Else	Restrict Acesss
	F4:Proceed()

If Encrypted key not valid, that means access is denied.

V. CONCLUSION

Secured M-cloud storage System is a multi-cloud storage system in cloud computing, which seeks to provide each customer with a better cloud data storage decision, taking into consideration the user budget as well as providing him with the best quality of service i.e. Security and availability of data offered by available cloud service providers. It shows ability of providing a customer with secured storage under his affordable budget. It holds an economical distribution of data among the available service providers in the market, to provide customers with data availability as well as secure storage. It provides a better decision for customers according to their available budgets.

REFERENCES

[1] A Secured Cost-effective Multi-Cloud Storage in Cloud Computing, Yashaswi Singh, Farah Kandah, Weiyi Zhang Department of Computer Science, North Dakota State University, Fargo, ND 58105

[2] Amazon.com, Amazon s3 availablity event: July 20, 2008, online at http://status.aws.amazon.com/20080720.html, 2008.

[3] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. Medard, Trusted storage over untrusted networks, IEEE GLOBECOM 2010, Miami, FL. USA.

[4] W. Itani, A. Kayssi, A. Chehab, Privacy as a Service: Privacy- Aware Data Storage and Processing in Cloud Computing Architectures, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec 2009.

[5] P. S. Browne, Data privacy and integrity: an overview, In Proceeding of SIGFIDET 71 Proceedings of the ACM SIGFIDET (now SIGMOD), 1971.

[6] C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, W. Lou, Privacypreserving public auditing for secure cloud storage, in InfoCom2010, IEEE, March 2010.

[7] A Study of Encryption Algorithms AES, DES and RSA for Security,Global Journal of Computer Science and Technology Volume XIII Issue XV Version I (D) Year E 2013

[8] Uli Kretzschmar, AES128 – A C Implementation for Encryption and DecryptioN, SLAA397A–July 2009–Revised March 2009