A Review on Secured Data Transfer with Multiple Clouds Using Blowfish Encryption

M. Narendran [1], B. Sai Praneeth [2], B. Sai Sumanth [3], M. Venkata Vijaya Rama Raju [4], S. Teja Venkata Rama Raju [5]
[1]Assistant Professor, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
[2,3,4,5] UG Scholars, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Abstract: - Cloud Computing is one of the required trending domain of the society as the public clouds are playing major role for data storage management using data centers. The present count of public clouds is increasing day by day for data storage requirement. The common interface for cloud is created through which the clouds can be accessed. The concept is to transfer the files of one personal cloud to other clouds of the same user and the transfer of the files from one user to other user clouds can also be done using a chat box as the common interface. The data will be transferred using the application database as an intermediary. The data in the intermediate database will be the encrypted form of original data. The data will be encrypted using the efficient technique and then transferred to other cloud. This multi cloud transfer helps the user to store the data in the most secured way.

Keywords—Data transfer, Chat room, BlowFish Encryption,

1. INTRODUCTION

Cloud storage services like Google Drive, Drop Box are a popular means for storing data and performing collaborative work. Personal cloud storage services are data-intensive applications on the Internet that allow the user to synchronize files with servers in the cloud and among different devices. The high public interest has pushed dozens of providers to the cloud storage market. New cloud providers have to compete against established ones such as Google, Microsoft, Drop Box, Box, which offer large amount of storage space for cheaper prices, while the high competition for customers continues to decrease the cost per GB, and the other important aspect is if synchronization, performance, and Quality of Experience (QOE), are mostly unknown given the proprietary design of most services. Thus, a detailed analysis has done to analyze the most efficient cloud. Transfer of files between the clouds is made possible using this application. A chat-based application is made which helps the multiple users to transfer files, messages between them. These files are stored in the respective cloud which makes the local space of the user free and maximum utilization of the cloud is made possible. This chat is highly encrypted using blow fish algorithm. Blowfish algorithm is a symmetric block cipher encryption algorithm which uses symmetric key to both encrypt and decrypt messages up into fixed length blocks during encryption and decryption.

Blowfish is a symmetric block cipher encryption algorithm meaning that it uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. This algorithm is used to encrypt the files that are transferred and the files in the one-to-one chat room are also encrypted.

2. RELATED WORK

A Review on Utilization of Memory Management Mechanism of Cloud Computing

Cloud storage services are a popular means for storing data and performing collaborative work. New cloud providers have to compete against established ones such as google, Microsoft, Dropbox which offer large amount of storage for cheaper price. Accessing all the clouds through a single platform and providing the efficient cloud by analyzing the features of respective clouds. So any one can use the analysis and upload the file in the efficient cloud and it also gives the user, the next efficient cloud among available clouds when the most efficient cloud is out of space. Some of the methodologies used in the clouds are bundling, chunking, compression, deduplication. This analysis is used as a reference to represent a efficient cloud and the drawback is there is no sharing of data between the clouds and the user. [1]

Spy Storage: A Highly Reliable Multi-Cloud Storage with Secure and Anonymous Data Sharing

In this paper, a design named Spy storage is proposed which offers highly reliable storage service and secured data sharing. Along with this multi cloud sharing mechanism was implanted using quorum protocol and by utilizing ABE/ABS cryptographic model. With the Extensive measuring experiments had proved that Spy storage can achieve a relative high reliability with low trade off of the file transfer speed. It integrates multiple cloud storage services to construct an overlay storage layer in order to overcome defects of single cloud storage services. This research is the first work using Attribute Based Encryption(ABE) and signature simultaneously in the multi cloud field to achieve a high reliable secure storage system with an easy sharing mechanism and optional anonymity service. [2]

Implementation Application Internal Chat Messenger Using Android System

At present the development of rapid communications equipment makes easier to communicate globally. Chat messenger application is used for android users to communicate through internet and have a chat such as line, WhatsApp, yahoo messenger and so forth. In communicating via instant messages, some people may also experience problems when communicating with foreigners, of which at least the required skills in the English language. The purpose of this research is to build the application chat messenger fellow android user through internal operation office. The result shows that the application can translate automatically in different language. [3]

Transfer Time-Aware Workflow Scheduling for Multi-Cloud Environment

In this paper an efficient workflow scheduling algorithm for multi-cloud environment is proposed which is based on transfer time consciousness. The proposed algorithm has two phases similar to Heterogeneous Earliest Finish time (HEFT) algorithm which was developed for multiprocessor system. The first phase calculates the B-Level priority of the tasks and second phase undergoes the virtual machines (VMs) selection based on the calculated B-level priority of the tasks. The results noticeably indicate that the proposed algorithm outperforms both the algorithms in terms of makes pan and average cloud utilization. [4]

Transfer time-aware workflow scheduling for multi-cloud environment

Workflow scheduling in a multi cloud environment is a challenging problem which is known to be NP-completing nature. The algorithm which is used in this has two phases similar to heterogenous earliest finish time(HEFT) algorithm which was developed for multiprocessor system. The first phase calculates the B-level property of the tasks and second phase undergoes the virtual machines(VMs) selection based on the calculated B-level priority of the tasks. The result noticeably out performs the existing algorithms in terms of make span and average cloud utilization. Here best available indicates that which VM makes minimum finish time of tasks. Task note prioritization demands the presidency of each task node to be calculated B-level priority value. The algorithm has shown to require O(n2m) time for n dependent tasks on m VMs. [5]

Cloud-to-cloud parallel data transfer via spawning intermediate nodes

This work proposes a parallel cloud-to-cloud data transfer method in which intermediate nodes are spawned and utilized in order to increase the transfer throughput by aggregating bandwidth. Existing data transfer methods do not take advantage of public cloud elasticity - the maximum throughput is limited by the available bandwidth of the source or/and destination transfer node. In this paper, a technique that does multi-part transfer by breaking down large files into smaller parts and transfer them in parallel via intermediate nodes is proposed. As intra DC bandwidth is often multiple times higher than inter DC or WAN, the proposed method allows transfer throughput higher than the bandwidth capacity of a single node. Based on modelling and experiment, the result shows that the proposed solution has potential to improve the overall performance. [6]

Ensuring an online Chat Mechanism with accountability to sharing the non-downloadable file from the Cloud

Cloud computing aims at allowing access to large amount of computing power in a fully virtualized manner, by aggregating resources and offering a single system view. More and more businesses and individuals are attracted by the benefits of the cloud and are shifting their data and computation work to be carried out in the cloud. But since the processing of user's data is done by remote computing resources and data is placed in remote storage systems, users of cloud computing has fear about the security of their data. These computation and storage are distributed in nature. To address this issue, a framework called Cloud Information Accountability. Hence this framework provides end to end accountability for user's data at both CSP and Cloud users by providing the log records for their data and also providing the online Chat mechanism which enables the CSP and Cloud users can communicate themselves to share file which is unable to download form the cloud. [7]

Enhanced Security for Multi Cloud Storage using AES Algorithm

The use of cloud computing has increased rapidly in most of the organizations. Security is considered to be the most important feature in a cloud computing environment because of the sensitive information stored in the cloud for users. The goal of cloud security is mainly to concentrate on the issues related to the data security and privacy features in cloud computing. The multi cloud model is based on data storage on distinct cloud by splitting files into different chunks then encrypts data using AES algorithm and MD5 technique is used for verification of data with two cloud servers. [8] A Study of Internet Instant Messaging and Chat Protocols. In this paper, Instant Messaging (IM) and internet chat communication have seen enormous growth over the last several years. IM is the private network communication between two users, where as a chat session is the network communication between two or more users. All the IM protocols allow authenticating with a central server, engaging in private messages and conversing in public chat rooms. Some IM systems allow file transfer, web cam usage, using privacy controls, maintaining buddy list, voice chat sessions. The two approaches used in this architecture are symmetric and asymmetric. In symmetric each

server performs identical functions, such that a client need not distinguish which server it contacts to engage in an activity. In an asymmetric approach each server is dedicated to a particular activity such as logging n, discovering other users in the network, maintaining a chat room or forwarding an instant message. [9]

3. PORPOSED MODELLING

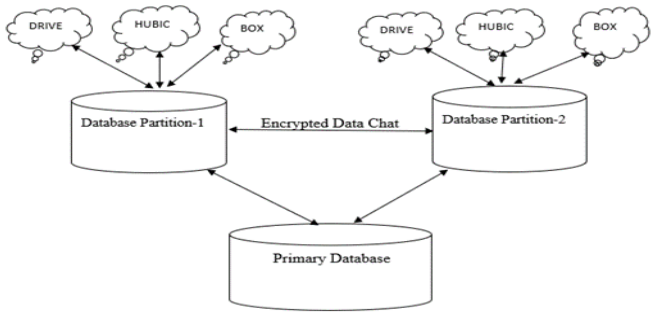

Fig: Architecture diagram

The architecture diagram explains the whole process of the system in which the encrypted data is transferred from clouds and also stored in a primary database linked to the user so that the storage in the systems can be saved. The data whether it can be content, photos, videos, files are encrypted with blowfish algorithm so that there is no chance of misusing the data by a third person.

4. RESULTS AND DISCUSSIONS

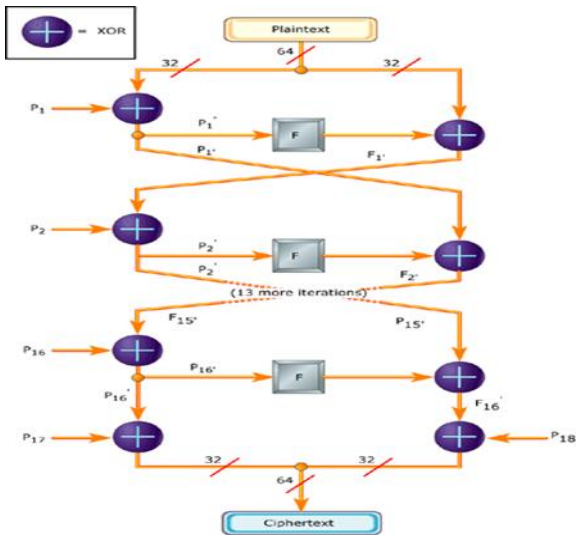

Fig: BlowFish Algorithm

The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It takes a variable length key, from 32 bits to 448 bits, making it ideal for securing data. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits.

There are two parts in this algorithm

A. Key-Expansion:

It will convert a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses large number of subkeys.

B. Data Encryption:

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

Every round r consists of 4 actions: First, XOR the left half (L) of the data with the r th P-array entry, second, use the XORed data as input for Blowfish's F-function, third, XOR the F-function's output with the right half (R) of the data, and last, swap L and R.

The F-function splits the 32-bit input into four eight-bit quarters and uses the quarters as input to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 232 and XORed to produce the final 32-bit output (see image in the upper right corner).[4]

After the 16th round, undo the last swap, and XOR L with K18 and R with K17 (output whitening).

Decryption is exactly the same as encryption, except that P1, P2, …, P18 are used in the reverse order. This is not so obvious because xor is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order).

Workflow Diagram

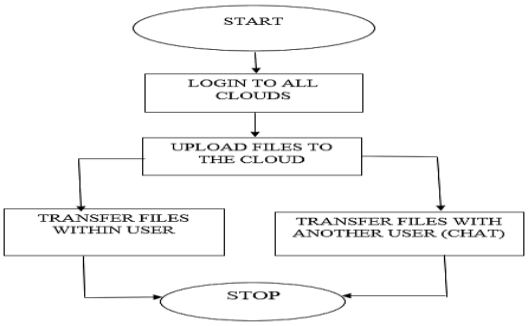

Fig: Workflow Diagram

The workflow of the system is explained in the diagram in which the user starts an application and login to the particular account then logs in to the clouds in which the account is existing. The files or any media can be uploaded to the cloud from this and also there is an option for transferring files from one cloud to another of the same user and there is a discussion forum which helps the user to transfer files to other user i.e., second person without downloading it from the cloud. The file will be downloaded into chat database but not the phone storage.

PROJECT OUTCOME

The project is developed mainly for the purpose of file transfer between the public cloud. Through this project had developed a better method for transferring the files between the clouds by saving the storage, data and time. For the information sharing chat box will be useful by which the communication becomes easier. The encryption also plays a major role in encryption through which it will provide a security firewall for file sharing. In an overview our project will be useful for file transferring, end-to-end encryption, chat box for information sharing, saves time, data and storage.

Parameters	**Existing System**	**Proposed System**
C 2 C File Transfer	Yes	Yes
File Transfer	Uses Local Storage	Uses Cloud Storage
Communication Between User	No	Yes
Encryption Type	AES	Blowfish
Data Transfer Limit	Up to 2 Users	Any number of Users

Table: Comparison of Existing & proposed system parameters

5. CONCLUSION

This paper concludes about the file transfer mechanism in between different public clouds. The user can transfer the files between the clouds without using the local storage. By this simple mechanism user can save a lot of time, memory and data. Here this model has a chat box in between the clouds through which the information about the file transfer can be shared. The user can have all the public clouds in a common interface, such that he can access all the public clouds at one place and the transfer of the files between the clouds will be done easily. For the security purpose of data base, this model provides an end to end encryption such that the sender and receiver only able to see the files that are transferred using the chat box as the mediator.

REFERENCES

[1] A Review on Utilization of Memory Management Mechanism of Cloud Computing
[2] Spy Storage: A Highly Reliable Multi-Cloud Storage with Secure and Anonymous Data Sharing
[3] Implementation Application Internal Chat Messenger Using Android System
[4] Transfer Time-Aware Workflow Scheduling for Multi-Cloud Environment
[5] Transfer time-aware workflow scheduling for multi-cloud environment
[6] Cloud-to-cloud parallel data transfer via spawning intermediate nodes
[7] Ensuring an online Chat Mechanism with accountability to sharing the non-downloadable file from the Cloud
[8] Enhanced Security for Multi Cloud Storage using AES Algorithm
[9] A Study of Internet Instant Messaging and Chat Protocols
[10] http://iitd.vlab.co.in/?sub=66&brch=184&sim=1147&cnt=1
[11] https://en.wikipedia.org/wiki/Blowfish_(cipher)