

Proneo: Large File Transfer using Webworkers and Cloud Services

Ms. S. Vidhya¹

PG Scholar, Department of CSE
Renganayagi Varatharaj College of
Engineering
Virudhunagar dist, India
vidhyanila@gmail.com

Dr. V. Ilankumaran²

Principal
Renganayagi Varatharaj College of
Engineering
Virudhunagar dist, India

Ms. R. Shanmugapriya³

PG Scholar, Department of CSE
Renganayagi Varatharaj College of
Engineering
Virudhunagar dist, India
rspriyait011@gmail.com

Abstract— Cloud computing is a term, which involves virtualization, distributed computing, networking, and web services. Efficient data transfer among the cloud server and client. Cloud storage enables users to remotely store and retrieve their data. In previous work, the data are stored in the cloud using dynamic data operation with computation which makes the user need to make a copy for further updating and verification of the data loss. The objective of our project is to propose the partitioning method & web workers for the data storage which avoids the local copy at the user side. The cryptography technologies offer encryption and decryption of the data and user authentication information to protect it from the unauthorized user or attacker. MD5 based file encryption system for exchanging information or data is included in this model. This ensures secure authentication system and hiding information from others. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data.

Index Terms— MD5, Data partitioning, Cloud Storage, Data Transfer.

I. INTRODUCTION

Cloud computing is an emerging topic in the field of parallel and distributed computing. This computing relies on sharing computing resources rather than having local servers or personal devices to handle application. Cloud Computing is a new computing model that delivers the computing missions on a pool that includes a large amount of computing resources. The development services are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) With broadband Internet access, Internet users are able to develop computing resource, storage space and software services. In cloud, large amount of various computing resources are placed in it, so users can easily find their solutions with the resources are provided by a cloud. This brings greatest elasticity for the users. Using cloud computing services, users can store their critical data in cloud server and can access their data from anywhere using the Internet. Users do not need to worry about system or disk crash.

In the cloud environment, resources are shared through servers, users and individuals. The files and data are stored in the cloud. Therefore, data or files of an individual can be handled by all other users of the cloud. One of the essential characteristics of cloud computing security is protecting integrity, availability and confidentiality of data stored in the cloud server. The Cloud Computing technology is embedded with three services which are just one click away, easy to use and pay as you use the service.

Cloud storage means the storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected

resources that comprise a cloud. Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware.

Cloud storage is a service for developers to store and access data in cloud. Cloud service provider will manage and control the cloud resources. Cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. Client uses the client devices to access a cloud system via World Wide Web. The benefits of the cloud storage are flexible with reduced cost and they also manage the data loss risk and so on. The data integrity checking protocol detects the data corruption and misbehaving server in the cloud storage.

In the proposed work Data partitioning technique, remote data integrity checking is analyzed in internal and external ways. MD5 concepts are used to check the integrity of data before storing of the data in cloud server. Admin maintain the user file list. Web Socket provides the connection to the server, and Base64 encoding allows the transfer of image data and these three technologies are used to send images to the browser in real-time. The new Web Socket API resolves the issue of sending data directly to the client by allowing the browser to maintain an asynchronous socket connection to a server. Servers can run on any computer including committed computers, which individually are also often referred to as the server. In many cases, a computer can supply several services and have

several servers running in the cloud storage. Servers are computer programs running to serve the requests of other programs to the clients.

II. RELATED WORK

In [1] the authors proposed cloud storage enables users to remotely store and retrieve their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Cloud service provider will manage and control the cloud resources. Client uses the client devices to access a cloud system via World Wide Web. The remote data integrity checking protocol detects the data corruption and misbehaving server in the cloud storage. The security mechanism is also emphasized in order to prevent unrecoverable data loss. MD5 concept are used to check the integrity of data before storing of the data in dacenter. AES algorithm are used to store end user client data for security and RSA are used for communication of secure cloud data for storing and retrieving process. The original data is complex and there is difficulty in storing it in cloud, so partitioning function is used to store the data in the cloud.

In [2] Downloading time is reduced using Bit Torrent application and Steiner tree algorithm. Bit Torrent, a popular Peer-to-Peer file sharing protocol for mass distributions. Steiner tree algorithm, a star based protocol to effectively reduce the distribution time. The main goal is to distribute data and reduce the distribution time using content distribution algorithms.

- Understanding Bit Torrent and Steiner tree algorithm.
- Host the Web application on the cloud.
- Write a simple Web based application and develop a System to achieve fast and minimum distribution time.

A Bit Torrent client is a computer program that manages downloads and uploads using the Bit Torrent protocol. Bit Torrent is for distributing large amounts of data over the Internet. Bit Torrent is one of the most common protocols for transferring large files The Bit Torrent protocol can be used to reduce the server and network impact of distributing large files. The problem is to find a Steiner tree connecting the source node and destination nodes that minimizes data distribution time. To minimizing upload and download time the Algorithm implemented is Bit Torrent and Steiner tree algorithm.

In [6] the authors proposed new security architecture for cloud computing system. Cloud also provides the ability to share and transfer large amounts of data in an efficient manner. This ensures secure authentication system and hiding information from third parties. In this a various light weight AES algorithm based cryptographic solution is proposed for optimizing security.

This model also includes onetime password system for user authentication process. Using cloud computing services, users can store their critical data in cloud data centers and can access their data from anywhere using the Internet. Two servers, computing server and authentication server are used here for ensuring high security. AES encryption algorithm is used for securing files. The MD5 hashing algorithm is used to cover the tables from users. One time password is used for authentication. The client has to make login to the server. One time password has been used to authenticate the user. An authenticated client encrypts the file by system's public key. The key is kept in the database table of the system server along with the user account name using MD5 hashing.

In [7] the authors proposed cloud FTP server on Windows Azure. There are two types of roles available: a worker role and a web role. Worker roles are frequently used for long-running parallel tasks that non-interactive. Worker roles are not constrained in the way they communicate with each other for each work role stands alone in a virtual server. A primary use is to allow web roles to communicate with worker roles, typically for notifications and to schedule work. The web roles are the front end to accept the user request, and then the task messages are written into the message queue and the worker roles reads from the message queue to take their jobs. Both web roles and worker roles take the storage service to store information.

FTP may run in active or passive mode, which determines how the data connection is established:

Active mode:

In active mode, the client creates a TCP control connection to the server and sends the server the client's IP address and an arbitrary client port number.

Passive Mode:

In passive mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server.

The users could upload and download files through ftp clients and the administrators could manage the cloud ftp through web portal. The worker role is responsible for transferring data.

III. PROPOSED WORK

We proposed web workers for reducing uploading and downloading time. Mini cloud will be created using web workers. In this, mini cloud will be created in client's browser page. Using multi thread technique, more than one web workers will be created. Each web workers are interconnected and managed by main service. Web worker

is an element in mini cloud it will share the work and it gets a small chunk of file and post it to given server address. Data is transferred among the server and client. Web Socket provides the connection to the server, and Base64 encoding allows the transfer of image data and these three technologies are used to send images to the browser in real-time. The new Web Socket API resolves the issue of sending data directly to the client by allowing the browser to maintain an asynchronous socket connection to a server.

MD5 algorithm is used for encryption. This ensures secure communication system and hiding information from others. Admin maintain the user file list. User works in two ways

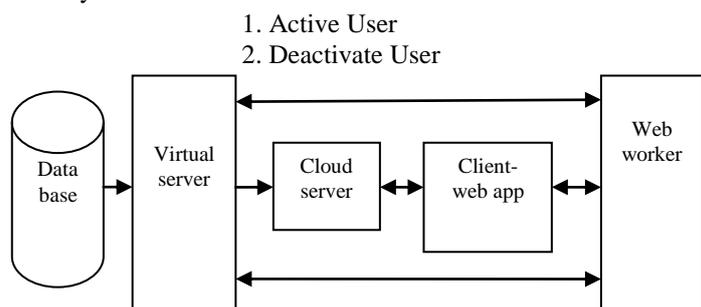


Figure1. System design of proposed work

A. User Login

In User Login, the new users are registered into the system by providing users information such as name, id, username, password etc. User Profile is generated in the Document DB with necessary details. If already registered users by entering the username and password user login to the system.

B. Admin

In an organization, admin create roles for users & also specify the number of file transfer per user as per their role.

C. Cloud Server

In cloud server to process the image generation then sending the image data to the client through the web browser. Server includes a large storage capacity and high-end graphics hardware. Server use Graphics processing units to process high-performance. The server is able to send data to the client at any time while the connection remains open.

A server is a storage space it contains lot of applications, files, information such as file size, file name. It also more capable of accept the requests from the client and immediately giving responses to the client. Servers can be used in any computer such as dedicated computers, shared computers. It is also referred to as the server.

Cloud Server can perform three operations like store file, get file, or file list. At the time of storing a file it get the file name, file size and domain name from request

message and sends a request to admin to store a file. At the time of receive a file to get the file name and file size from request message and send a request to storage admin to get a file. To delete file to get the file name and send a request to storage admin and it also show the file list according to client request send to storage admin.

Servers are computer programs to run and serve the requests of other programs to the clients. Thus, the server performs some computational tasks on behalf of clients. Some facilitates are in clients such as share data, information or any hardware and software resources. The server is able to send data directly to the client without the constant polling from the client for new updates.

D. Client

Client needs to create a connection to receive image data from the server and then display it to the end-user. In this module use HTML5, web socket API, Base 64 image encoding. HTML5 allows image data to be displayed to the user's screen. Web Sockets provide the connection to the server, and Base64 encoding allows the transfer of image data these three technologies are used to send images to the browser in real-time.

The new Web Socket API resolves the issue of sending data directly to the client by allowing the browser to maintain an asynchronous socket connection to a server. By maintaining this connection, the client is able to instantly send data to the server without needing to re-establish a connection. The client's browser asks the cloud server for a resource, and the server responds by sending the resource and closing the connection.

The basic operations of how a client uploads/downloads files to/from the cloud.

File Upload

In the file upload operation the client first encrypt the file with MD5 algorithm by attaching files to it.

File Download

In the file download operation the client fetches the file from the cloud server.

E. Authentication

The Web Socket API defines a simple protocol to transfer information, and provides a method for creating secure connections which is beneficial for authentication purposes. Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. Authentication is the process of actually confirming that identity.

F. MD5 Message Digest Algorithm

MD5 message digest algorithm is also used for encrypt the messages and password. In this algorithm takes a message as input and it also produces an encrypted output.

It contains 128 bit message. The MD5 algorithm is also intended for many applications, where a huge file must be digested in a secure manner. MD5 is an algorithm that is used to check the data integrity through the creation of a 128 bit message digest from the input information. It is also used in much software to give assurance for file transfer.

G. Partitioning Data

Partitioning function also plays an important role in this work. It blobs huge files into small chunks to store the data in easy manner and also easy to access the data when there is need. The original data is very complex and store the data in cloud is also very difficult, so blob function is also used and easy to store the data in the cloud.

IV. EXPERIMENTAL RESULTS

Different Timing was observed during the working and processing of this proposed model.

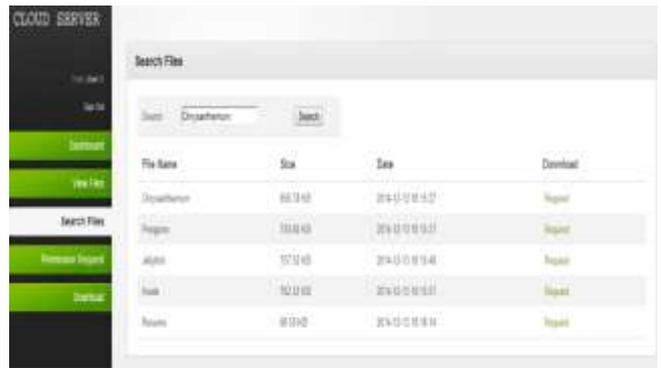


Figure5.Represents the downloading procedure

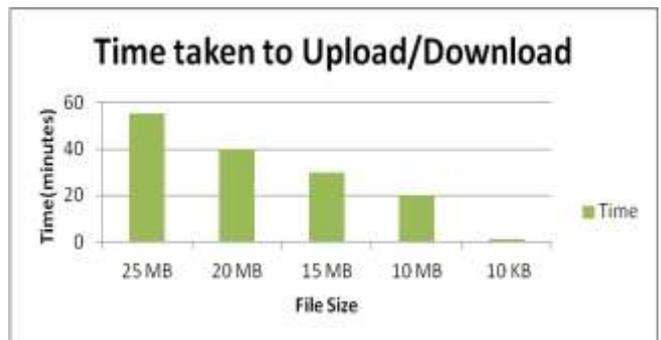


Figure6.File upload and download time



Figure2.Represents the uploading procedure

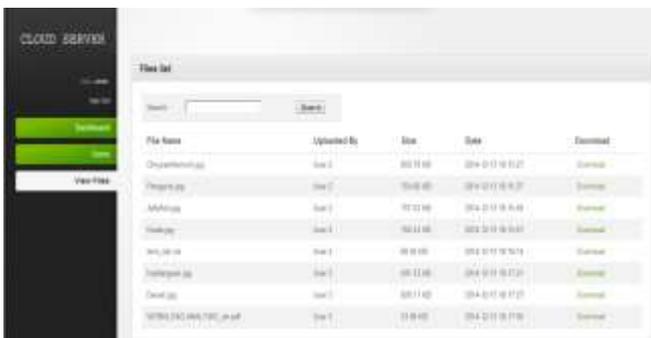


Figure3.Represents file list for download process



Figure4. Representation for permission request

V. CONCLUSION

In this paper, we propose a large file transfer in cloud service. The blob function information enables store the data in easiest and effective manner. It also gives a way for various accesses and there is less cost to store the data. The time is also effectively reduced during upload and download process because the use of web workers. Finally we have to store their data on a cloud without worrying about the data integrity. It also ensures the data security.

VI. FUTURE WORK

In our future work we proposed dedicated web worker for client side. Dedicated web worker compute heavy processing. It also improves the system performance

ACKNOWLEDGEMENT

The Authors are willing to express their profound gratitude and heartiest thanks to all the researchers in the field of cloud computing architecture's security.

REFERENCE

[1] Swap nil V.Khedkar, A.D.Gawande, and "Data Partitioning Technique to Improve Cloud Data Storage Security", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 3347-3350, 2014.

- [2] S.Priyanka, R.Kalpana, and M.Hemalatha, "Reducing upload and Download Time on Cloud using Content Distribution Algorithm," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, pp. 101–105, 2013.
- [3] Rajiv Kumar Ranjan, Dimpi Rani, "Enhance Data Security of Private Cloud Using Encryption Scheme with RBAC", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014.
- [4] Iranna Telasang, Manjunatha Dai Mao, "A Secure Cloud with Additional Layer Of Protection and User Authentication," International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, June 2013, pg.307 – 313.
- [5] A.Venumadhav, "Assured Data Transfer under Auditing in Distributed Circumstances," International Journal of Advanced Research in Computer Science and Software Eng. 4(3), March - 2014, pp. 1087-1090.
- [6] Lalit Gehlod, Vishal Deep Rathore, "An Enhanced Authentication Architecture for Cloud Computing System," International Journal of Engineering Sciences & Research Technology [272-279] June 2014.
- [7] Ch.Madhu Babu, O.Lakshmi Chandana, "File Transfer Protocol in Cloud Computing," International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 3
665 – 667 March 2014.
- [8] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, M. A Hashem "A Newer User Authentication, File Encryption and Distributed Server Based Cloud Computing Security Architecture" International Journal of Advanced Computer Science And Applications, Vol. 3, No. 10, 2012.
- [9] T. Niranjan Babu, G. Siva Shankar, "An Approach for Security and Privacy Enhancing By Making Use of Distinct Clouds", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-2, and May 2014.
- [10] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M.Salem," Cloud Computing Cryptography State-Of-The-Art", International Journal of Computer, Information, Systems and Control Engineering Vol: 7 No: 8, 2013.