International Journal of Scientific Research and Engineering Development-– Volume2 Issue 2, Mar –Apr 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

EFFICIENT FILE DOWNLOAD TIME REDUCTION SYSTEM FOR MULTI-CLIENT FOG/CLOUD ENVIRONMENT

Ms.S. Srimadhura *, Mrs.R.Sudha**

(S.Srimadhura, M.E,.Dept of computer science, Arasu Engineering College, Kumbakonam ,India)
** (R.Sudha, Assistant Professor ,Dept of computer science, Arasu Engineering College, Kumbakonam ,India)**

----------**********----------

Abstract:

The concept is decreasing the download time of various records asked for by numerous customers from different cloud/mist stockpiling servers. Given conceivable past document downloads by the customers, organize coding can be productively abused to assist the download procedure. Since every customer can tune to just a single server at any given moment, the arrangements of customers served by the diverse servers must be disjoint so as to ensure a most extreme decrease in download time. To achieve disjoint download systems, a double clash organize coding chart is proposed. Given the immovability of the long haul ideal arrangement, we propose an online calculation utilizing the structured double clash diagram. For the instance of one record ask for per customer, both asymptotic lower and upper limits of the execution of the proposed strife free calculation are inferred.

Keywords **— Cloud Computing, Data transfer, Multi user, Fog computing, Multi file**

----------**********----------

I. INTRODUCTION

IN the most recent decade, an exponential development of capacity frameworks limit has been seen as the requirement for putting away messages, photographs and recordings expanded. This development empowered the advancement of new information stockpiling strategies so as to improve the two noteworthy execution pointers of information stockpiling frameworks, to be specific unwavering quality and availability [2], [3]. To this end, distributed storage frameworks, in which records are put away in numerous server hubs with suitable reiteration (and potentially coding), developed as a reasonable answer for move forward the accessibility and unwavering quality of capacity frameworks [2], [4]. Distinctive dispersed capacity procedures were proposed in the writing for this worldview to enhance the framework unwavering quality. One procedure is full replication of similar information in various capacity units, which forces incredibly high capacity overhead. Another technique that can give better excess unwavering quality exchange off is eradication/organize coding intended to secure information against incomplete

information misfortune occasions [2], [3], [4], [5], [6]. In contrast to framework dependability, the framework availability issues (i.e., issues with respect to customers of a system getting to and downloading their asked for records in a proficient way) are less concentrated in the writing. An availability display with tree structure, comprising of a line associated with a lot of capacity servers that gets customer demands and calendar their download, was proposed in [7]. In spite of the benefits of this methodology, it didn't think about two commonsense parts of distributed storage frameworks. To start with, the point-to-multipoint show considered in this work restricts the possibilities of distributed storage servers to work in a multipoint-to-multipoint mold.

To be sure, the various solicitations of various customers can be served all the while from the diverse cloud servers. Second, it overlooks the likelihood of earlier record downloads by the customers from the cloud servers. These earlier downloaded documents, if exist, can be utilized as side data to essentially diminish the download time of the present customer asked for documents utilizing system coding. On another note, the wide spread utilization of the advanced mobile phones has brought about an enormous barged in substantial rush hour gridlock request (essentially video content) from 4G cell base-stations. The expected enormous development in such requests can't go on without serious consequences with the current cell arrange designs. This challenge prompted the rise of mist radio access systems (F-RANs), as a potential competitor design for 5G cell systems [8], [9], [10]. F-RANs were enlivened by late examinations indicating both a high and moderate fluctuating worldly relationship among the video traffic requested by end-customers. This fascinating finding propelled the possibility of proactively (i.e., without client ask for) storing of such "mainstream" documents in a "mist" of capacity units near the end-customers, which could be finished with low rates or in off-top occasions of the macrocell base-stations. The customers would thus be able to get to these records from these mist stockpiling system consequently offloading this sort of substantial load traffic from the macrocell base-stations

Cloud computing is hot trending, commercially gaining and flexible environment for providing online services for the Client over the Internet. The Client can register on cloud and access the cloud services for free or by pay per service manner. In cloud environment there is no need for the physical system implementation web servers, database servers and file servers can be implemented virtually [2]. There are many cloud services like data sharing, data storage, database storage and online applications are provided by some service providers. The consumer who are the clients are provided with the client side application or online account to access their permitted services. Web

browser, mobile application and desktop application are some client side access to the cloud. The consumers are allowed to access the web services remotely from anywhere via the Internet services. It is the responsibility of the cloud service providers to provide flexible, secured, efficient, accurate and timely services to the client.

Presently we are lies in the era of computer. Computer is ruling the world. It is everywhere where we go. Also consumers of cloud network are becoming high [1]. There are 3,424,971,237 of consumers using the Internet everyday around world. It is 46.1% of world population consuming Internet in their everyday use. So there are such a number of services accessed from the cloud everyday. The service providers has to preserve access control for the client access and should provide access only to those eligible users. A better access control and authentication scheme should be implement on the cloud network. A user should authenticate himself before accessing a service from the cloud [3]. The traditional way of authenticating client using username and password is no more secure due to the advanced technique of hackers like key logging and phishing pages attacking [22]. But it can also consider as one of the parameters of authentication [5]. Another method of recent day authentication is device based and application based authentication. The consumer is allowed to access cloud services only from the desired software application. The consumer has to authenticate himself from that software application as the first stage. Then the service provider will validate the software application by its ID. But there are many fake malicious applications are developed by the hackers to spoof the service providers and the clients. So the traditional attribute based authentication scheme is no more valid for recent malicious environment.

II. LITERATURE SURVEY

Several review work is done on different type of authentication scheme used on recent days. They are discussed one by one.

2.1 An Authenticated Trust and Reputation Calculation

It authenticates the Cloud Service Provider and Sensor Network Provider [1]. It also sets attribute requirements of the cloud service provider and cloud service user to access the web. It calculates the trust and reputation regarding the service of cloud service provider and Sensor Network Provider [25][28]. It helps the Cloud Service user to choose desirable Cloud Service Provider by assisting the Cloud Service Provider selecting Sensor Network Provider.

2.2 Smart Card Generator

This scheme includes three phases system setup, registration and authentication. The Smart Card Generator first setup the master private key by generating a random number. And then computes the corresponding public key and attributes. Then it publishes public key and public parameters. The

consumer can utilize the public key for accessing purpose. The service provider and the consumer has to register with the SCG [2]. The identities were sent to the service provider and the consumer. These identities is later verified for the access control. The identity based cryptosystem is used to encrypt and decrypt the user data over the cloud.

2.3 Location-based arbitrary-subspace skyline queries

This paper concentrates on Location Based Service authentication. Merkle Skyline R-Tree is used to process the queries. Partial S4-Tree is used for the authentication purposes [3]. Pre-fetched based approach is used to identify and authenticate location of the consumer. The query validation and revaluation is done periodically on the server. The authentication problem is processed using subspace and arbitrary processing. It enables authentication for large dataset and for large subspaces. But this scheme failed to extent the work to networking model. The skyline process may not work in large network environment.

2.4 Authenticating k-nearest neighbor

This paper studies the problems in query verification on road networks [4]. This paper proposes network Voronoi verification scheme. The Voronoi cell is considered as the object to verify correctness and completeness of the queries. It reduces verification cost on mobile user by using Improved Distance verification model [23]. This verification model can support recent features in the mobile computing network. This paper can extend to work on more spacial regions. It is capable to support only one data-owner.

2.5 Cloud Centric Multi-level Authentication

It uses hierarchical authentication scheme of IOT devices on cloud network. It improves scalability on safety responsibility. It offloads continuous authentication and lightweight implementation [5]. It enables two level authentication on wireless sensor networks. This enables easier mobility management over the network. Elliptic Curve Cryptography is used for key encryption scheme [19]. Elliptic Curve Diffie Hellman algorithm is used for key exchange. Elliptic Curve Cryptography Digital Signature is used for digital signature generation. It is used for authenticating secret messages over the network.

2.6 Public Integrity Auditing for Cloud Sharing

It supports multi-user data sharing and modifications over the cloud. The protocol is very secured to implement and working [6][14]. But it fails to prove soundness and semantics of the implementing formula [26]. It revokes the client if not valid via third party auditing.

2.7 Anonymous and authentic data sharing system

It allows data-owner to authenticate anonymously and put into cloud storage for analysis. It is scalable for certificate verification for public key infrastructure [8]. It eliminates certificate based key verification using ID based

ring structure. The secret key of the user and the digital signature that generated previously treated as an individual terms. This process eliminated data-owner re-authentication for every data. This scheme proves security pattern in low cost scheme.

2.8 Decentralized access control scheme

It supports anonymous authentication in cloud network. Without knowing the user identity the cloud authenticates the user data. It also provide access control which only valid user can decrypt and store data [9][15]. This scheme prevents the cloud from the reply attacks. This scheme is decentralized and robust. It supports communication, computation and proper storage.

2.9 Public Audibility and Data Dynamics

This paper achieves public auditing and Dynamic data processing [10]. It first verifies difficulties and potential security in doing this. Classic merkle hash tree construction is used for authenticating data on cloud [16]. Bilinear aggregate signature is used for multiple auditing. Third party auditing tool is used for multiple auditing simultaneously [17]. This system is highly secure and provable.

2.10 Object Centered Approach

It process the logging mechanism also with user policies and services [18]. Dynamic and traveling object is created for triggering access control and authentication that performed automatically on local [11]. This method proves efficiency and effectiveness of the system.

2.11 Role Based Cascaded Delegation

It supports simple and effective authority delegation over the servers on the cloud [12]. It enables user to create delegation rules based on his collaboration. This delegation role is verified by the administrative role [21]. The aggregated signature is used for authentication based on delegation rule.

2.12 k -times Attribute-Based Anonymous Access Control

Used to authenticate user anonymously on the cloud [13]. The cloud only knows about the attributes of the user not the ID of the user. These attributes are set with some limits and it is used to limit the users from some access. This scheme is proved as the practical one.

III. METHODOLOGY:

An online calculation utilizing the structured double clash chart. For the instance of one record ask for per customer, both asymptotic lower and upper limits of the execution of the proposed strife free calculation are derivedFirst, the point-to-multipoint display considered in this work confines the possibilities of distributed storage servers to work in a multipoint-to-multipoint mold. To be sure, the various solicitations of various customers can be served all the while from the distinctive cloud servers. Second, it disregards the likelihood of earlier record downloads by the customers from the cloud servers.Multipoint-to-Multipoint framework and its impact on the general download time problem.The proposed double clash IDNC

approach takes out all such transmission strife occasions totally, along these lines completely using the gain of expanding the customers' side data measure. It has five phases

- Data Owner Upload Files
- Store The Data
- View User details and file details
- Accessing Cloud file by User
- Download file by multiple user or multiple file by single user

Phase-1:

The information proprietor picks the record to transfer in the cloud. At that point they produce key to encode the information for anchored stockpiling. The information proprietor at that point encodes the information utilizing the key. Subsequent to encoding the information, the proprietor transfers the scrambled records in the cloud.

Phase-2:

The information proprietor store the encode information for anchored stockpiling and transfers records for information lump pressure of decode key. Distributed storage has a few gives over the conventional information pressure stockpiling.

Phase-3:

The data owner can view the all registered user and also can view the all files

Phase-4:

The client demands for looking record to information proprietor. Client can just view the pursuit document. The scrambled record organize is seen to the client. At that point, the client unscrambles the record by key given by client. At that point the client can see the first documents

Phase-5:.

Various solicitations of various customers can be served at the same time from the distinctive cloud servers. In this module different client or customer can download the single document from the haze or might be the single client download the numerous record by utilizing strife free calculation in this both procedure download time will diminished at the same time. Reenactment results demonstrate this proposed calculation shows close ideal execution contrasted with the ideal arrangement, and a critical decrease in download time when contrasted with the per-server organize coding plan.

Algorithm:

while true:

wait for authentication

get UI from client

get password from client

get db_password for UI

if db_password = password

generate single file

send _file

else

while true:

get UI and session_key

get_all UI list

for id in UI_list

if id=UI

generate multiple file

send multiple file

else

received by multiple user

end for

invalidate_client.

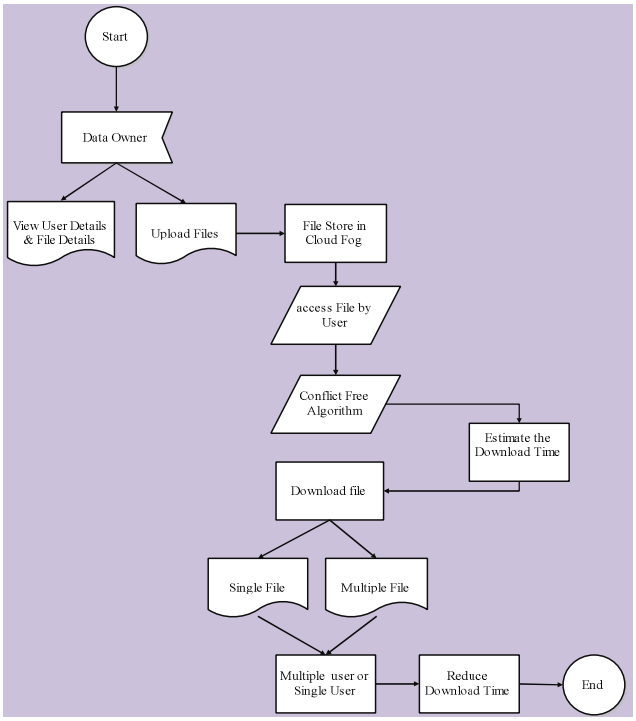
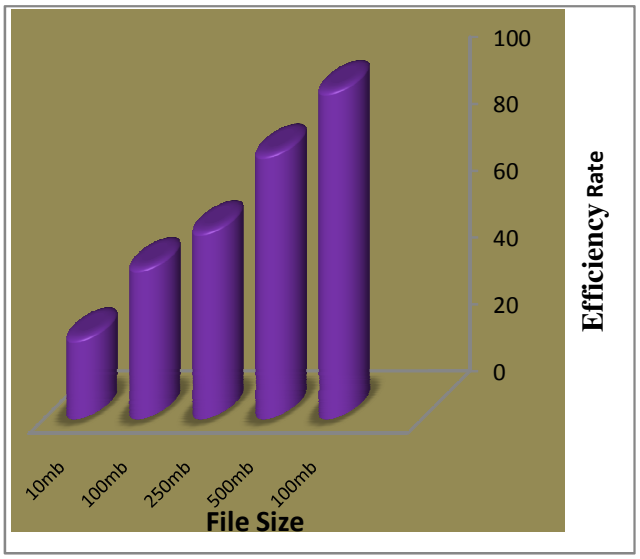


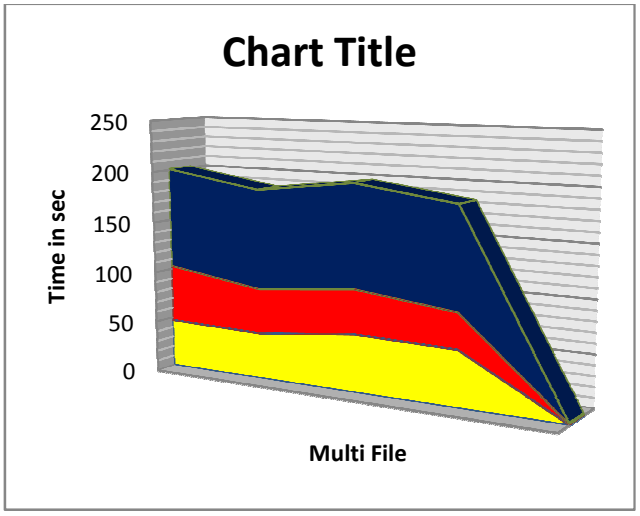
Fig.1. Work Flow

IV.RESULT AND DISCUSSIONS:

In this area, we look at, through broad reproductions, the execution of our proposed technique calculation to that of the customary of viewing multiple files to multi user in a less time and the efficiency is estimated to limit the download time without considering the solicitations served by alternate servers. We think about two cases for the criticism channels(the channels between the servers and the customers) to be specific, immaculate criticism and flawed input channels.



Graph.1. Efficiency File Transformation to user



Graph.1. Efficiency Comparison with Existing algorithm

V.CONCLUSION

The multi-client download time reduction problem from cloud/fog storage servers was investigated in

perfect and imperfect feedback environments. Applying the conventional PMP IDNC algorithm at each server separately was shown to result in transmissions conflicts, which reduced the download efficiency. Consequently, A novel dual-conflict graph model that avoids such conflicts and guarantees conflict-free trans- missions. The download time reduction problem was first formulated as an SSP problem and shown to be intractable. We thus designed an online heuristic algorithm that applies maximum weight vertex search over the dual- conflict graph to find the most suitable file download pat- tern at DTU. For the special case of lossless-channels, fixed storage model, and one file request per client, an upper and lower bounds of the conflict-free IDNC algorithm performance were derived. The simulation results show that this bounds are valid for both fixed and random storage models,The proposed algorithm was also shown to achieve near optimal online performance.

VI. REFERENCES:

[1]. 3GPP: Network architecture. TS 23.002, 3rd Generation Partnership Project (3GPP) (Sep 2008)

[2]. Aazam, M., Huh, E.N.: Fog Computing and Smart Gateway Based Communication for Cloud of Things. In: Proceedings of the 2014 International Conference on Future Internet of Things and Cloud. pp. 464–470. FICLOUD'14, IEEE Computer Society, Washington, DC, USA (2014) 35

[3]. Abramova, V., Bernardino, J.: NoSQL databases: MongoDB vs Cassandra. In: Proceedings of the International C* Conference on Computer Science and Software Engineering. pp. 14–22. C3S2E '13, ACM, New York, NY, USA (2013)

[4]. Abramova, V., Bernardino, J., Furtado, P.: Evaluating Cassandra Scalability with YCSB, pp. 199–207. Springer International Publishing, Cham (2014)

[5]. Anwar, A., Cheng, Y., Gupta, A., Butt, A.R.: Mos: Workload-aware elasticity for cloud object stores. In: Proceedings of the 25th ACM International Symposium on High-Performance Parallel and Distributed Computing. pp. 177–188. HPDC '16, ACM, New York, NY, USA (2016)

[6]. Balouek, D., Carpen Amarie, A., Charrier, G., Desprez, F., Jeannot, E., Jeanvoine, E., Lebre, A., Margery, D., Niclausse, N., Nussbaum, L., Richard, O., P´erez, C., Quesnel, F., Rohr, C., Sarzyniec, L.: Adding Virtualization Capabilities to the Grid'5000 Testbed. In: Ivanov, I., Sinderen, M., Leymann, F., Shan, T. (eds.) Cloud Computing and Services Science, Communications in Computer and Information Science, vol. 367, pp. 3–20. Springer International Publishing (2013)

[7]. Benet, J.: IPFS - Content Addressed, Versioned, P2P File System. Tech. rep., Protocol Labs, Inc. (2014)

[8]. Bonomi, F., Milito, R., Natarajan, P., Zhu, J.: Fog Computing: A Platform for Internet of Things and Analytics, Studies in Computational Intelligence, vol. 546. Springer International Publishing (2014)

[9]. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog Computing and Its Role in the Internet of Things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. pp. 13–16. MCC '12 (2012)

[10]. Brand, G.B., Lebre, A.: GBFS: Efficient data-sharing on hybrid platforms: Towards adding WAN-wide elasticity to DFSes. In: Computer Architecture and High Performance Computing Workshop (SBAC-PADW), 2014 International Symposium on. pp. 126–131 (Oct 2014)

[11] Roberto Tamassia, Fellow, IEEE, Danfeng Yao, Member, IEEE, and William H. Winsborough, "Independently Verifiable Decentralized Role-Based Delegation", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 6, NOVEMBER 2010.

[12] Tsz Hon Yuen, Joseph K. Liu , Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou, "k -times Attribute-Based Anonymous Access Control for Cloud Computing", IEEE Transactions on Computers, 2013.

[13] Shuanghe Peng, Zhige Chen, Deen Chen, "Membership Proof and Verification in Authenticated Skip Lists Based on Heap", S ECURITY S CHEMES AND S OLUTIONS, 2016.

[14] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, Senior Member, IEEE, and Jinjun Chen, Senior Member, IEEE, "MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud", IEEE TRANSACTIONS ON COMPUTERS, 2013.

[15] Igor Faynberg, Hui-Lan Lu, and Herbert Ristock, "On Dynamic Access Control in Web 2.0 and Beyond: Trends and Technologies", 2011.

[16] Jin Li, Xiao Tan, Xiaofeng Chen, Duncan S. Wong, Fatos Xhafa, "OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices", IEEE Transactions on Cloud Computing, 2013.

[17] Jiawei Yuan, Shucheng Yu, Member, IEEE, "Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification", IEEE Transactions on Information Forensics and Security, 2013.

[18] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael Calvo, "SafeProtect: Controlled Data Sharing with User-Defined Policies in Cloud-based Collaborative Environment", JOURNAL OF L A TEX CLASS FILES, VOL. 11, NO. 4, DECEMBER 2012.

[19] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti, "Scalable architecture for multi-user encrypted SQL operations on cloud database services", IEEE Transactions on Cloud Computing, 2013.

[20] Fei Chen, Tao Xiang, Yuanyuan Yang, and Sherman S. M. Chow, "Secure Cloud Storage Meets with Secure Network Coding", IEEE Transactions on Computers, 2015.

[21] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram, "Secure Logging As a Service—Delegating Log Management to the Cloud", IEEE SYSTEMS JOURNAL, 2011.

[22] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, "Security Challenges in Vehicular Cloud Computing", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1, MARCH 2013.

[23] Honggang Wang, University of Massachusetts Shaoen Wu, Ball State University Min Chen, Huazhong University of Science and Technology Wei Wang, South Dakota State University, "Security Protection between Users and the Mobile Media Cloud", IEEE Communications Magazine, March 2014.

[24] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, 2013.

[25] Slawomir Grzonkowski and Peter M. Corcoran, Fellow, IEEE, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", IEEE Transactions on Consumer Electronics, Vol. 57, No. 3, August 2011.

