# A NOVEL APPROACH FOR EFFICIENT DATA HANDLING IN CLOUD ENVIRONMENT

Sanchana. V. B., Renuga S. and M. Saravanan
Department of Computer Science Engineering, Faculty of Computing, Sathyabama University, Chennai, India
E-Mail: sanchanasundaresan19@gmail.com

## ABSTRACT

Information prefetching is a method on the breaking point servers in suitable file frameworks for scattered figuring. The prefetching file data about customer focus focuses is piggybacked onto the true customer input/output asking for, and a while later sent to the corresponded stockpiling server. The prefetched data can be pushed to the related client machine from the purpose of restriction server. Prefetching system can benefit went on file structures for cloud circumstances to fulfill better input/output execution. The part first request about plate input/output tracks to suspect the future circle input/output get to so that the limit servers can bring data early, and starting now and into the foreseeable future the prefetched data to basic client file systems for future potential occupations. In this paper, we proposed a thought to get cloud record scattered the prefetched data to the key client machines proactively. The data about customer focuses is piggybacked onto the true blue customer input/output asking for, and after that sent to the essential stockpiling server.

**Keywords:** cloud computing, data prefetching, piggybacking, distributed file systems.

## 1. INTRODUCTION

Distributed computing is “set of assets and administrations offered through the Internet”. “Cloud administrations are conveyed from server farms situated all through the world”. Plainly, security is a genuine worry in such a major domain. Cloud administrations can be executed utilizing diverse methodologies and advancements which should be secured at the distinctive phases of the solicitation/reaction cycle between customers (depending gatherings, for example, clients or applications) and administration suppliers (organizations or divisions inside of an organization uncovering those administrations). A few security layers are characterized in the middle of customers and administrations suppliers. The primary security layer, otherwise called "edge security" or "first line of resistance," is alluded to as the neutral territory or DMZ. The second security layer, or "green zone" to proceed with the military similarity, is situated behind the inward firewall of the DMZ. Now and again, the green zone might incorporate a few security sub-layers intended to further channel access to web administrations. At long last, the last security layer which we are centering at, or "last-mile security," is given by operators co-situated with the web administrations or applications to be ensured.

"Privacy is characterized as the confirmation that touchy data is not unveiled to unapproved persons, procedures, or gadgets." Cloud figuring frameworks give different Internet-based information stockpiling and administrations. Because of its different advantages, which incorporate cost viability and high adaptability and adaptability, distributed computing has increased noteworthy accomplishments as of late as another worldview for disseminated registering for different applications. With the quick development of the Internet, administration arranged design (SOA) and virtualization innovations, distributed computing prompts the vision of Internet as a supercomputer. Be that as it may, distributed computing has a noteworthy constraint to be comprehensively received because of the genuine obstruction that present distributed computing frameworks can't shield the classification of clients' information from their administration suppliers. A late overview demonstrates that the greater part of cloud clients expect that their information is being stolen and abused or altered. Data security is reliably a crucial piece of nature of organization and it is furthermore a key issue in disseminated registering. The data set away in cloud is standing up to different and neoteric challenges. Starting late, the criticalness of ensuring the data security in conveyed registering has been highlighted by authorities and endeavors.

Conveyed capacity depends on the framework preparing environment. There are various focal points to move data into the cloud. Case in point, customers need not consider the complexities of direct hardware organization. In any case, since customers store their data in the cloud, it suggests that they will lose control of them and more concerns will rise about the data security. The Security techniques have a couple purposes of hobby. In any case, it offers puzzle to encoded data which are secured with no attempt at being subtle fogs. Second, it offers controlled data get to and sharing among customers, so that unapproved customers or untrusted suppliers can't get to or look for over data without customer's endorsement. Shockingly, notwithstanding its favorable circumstances, distributed storage brings a few security issues. Information confidentiality shows up as the greatest sympathy toward clients of a distributed storage framework. Indeed, the customers' information is overseen out of their administration. Kamara *et al*, [1] and Chow *et al*, [2] concurred that encoding outsourced information by the client is a decent distinct option for moderate such worries of information confidentiality. In this way, the client safeguards the decoding keys outside of anyone's ability to see from the administration supplier, to be specific with the client himself. The confidentiality provisioning turns out to be more perplexing with flexible information accessible. It requires efficient sharing of decoding keys between different approved clients. So that, just approved clients can acquire the reasonable content of information put away in the cloud. In this paper, we depict another strategy for enhancing information confidentiality in distributed storage frameworks and upgrading dynamic sharing between clients. It can be utilized by a validated client for his information stockpiling. A representative solution for ensuring data safety in keeping the encrypted data in cloud storage with two-key encrypted system is introduced with a key generator system in the service provider to avoid any threats in cloud storage.

## 2. REVIEW OF LITERATURE

Puttaswamy *et al*, [3] implemented four strategies to enhance the information secrecy at the season of information being put away on outsider figuring. The principal strategy was to distinguish all practically encryptable information for encryption. The touchy information was to be scrambled without constraining the usefulness of the cloud application. It was to minimize key administration multifaceted nature at the season of guaranteeing heartiness while trading off the key. The fourth strategy was to give straightforward of information access so as to keep from malevolent mists at the client gadget. Tribhuwan *et al.* [4] proposed a technique to upgrade the security of information put away in the cloud by using the idea of homomorphic tokens and disseminated confirmation of deletion coded information. This technique accomplished both the joining of capacity accuracy protection and information mistake areas. They presented another two way handshake plan which depends on the token administration technique. This strategy does not work legitimately to maintain the uprightness and privacy of information.

Sato *et al.* [5] recommended one of the security attentiveness toward cloud that could be condensed as social in security. It was ordered into the different partner issues, the open space security issue and the mission basic information taking care of issue. As an answer of these issues, they proposed another cloud trust model. They considered both inside trusts display and contracted trust show that could control cloud administration suppliers. They introduced a model named as "Security Aware Cloud" Seung-Hyun Seo, *et al* [6] proposed the intervened certificateless open key encryption without utilizing matching operations. While matching the delicate information, there emerge the key escrow issues. At the point when not matched, the delicate information are in part decoded upon the fruitful approval and the remaining information are unscrambled by the client. This plan enhanced the proficiency of encryption of the information which diminished the computational overhead by utilizing matching free approach. The upsides of this plan are that the key Generation Center lives at open mists. It tackles escrow issue and repudiation issue and guarantees secrecy of information put away in broad daylight cloud.

Jeong-Min [7] highlighted the late study model utilizing Key Policy-Attribute Based Encryption (KP-ABE) and Proxy ReEncryption (PRE). The aforementioned both models abused the privacy of information through blending assault of disavowed clients in framework. This paper proposed a model that would store and separation the information record into header and body. It designated the decoding right by utilization of Type-based Proxy reencryption. It separated information records put away on cloud servers as header and body and had the unscrambling rights as head (scrambled key utilizing KP-ABE) and body (encoded message utilizing symmetric encryption).

The rule center is on the suitable utilization of the virtual machines and adjusting the virtual machines with the moving nearer asking. Load adjusting is depicted as a strategy for reassigning to make productive asset use the aggregate weight to the individual focuses of the aggregate framework and consequently minimizing under or over use of the open assets or virtual machines [8]. Shridhar et.al, [9] have made Modified Throttled figuring which keeps up a record table of virtual machines additionally the condition of VMs, for example, the Throttled tally [10]. There has been an attempt made to enhance the reaction time and complete gainful usage of accessible virtual machines.

Need chooses the centrality of the part with which it is connected. To the extent errand booking, it chooses the solicitation of task arranging considering the parameters grasped for its estimation [11]. In the present structure, the due date develop assignments are sorted out concerning the reason of errand due date. The errands with shorter due date ought to be executed first. So they are given more need in booking gathering. The endeavor once-over is balanced with assignments sorted out in rising solicitation of due date remembering the deciding objective to execute the errand with minimum time necessity first. The cost develop endeavors are sorted out concerning the reason of task advantage in dropping solicitation. This is measurable as assignments with higher advantage can be executed on minimum cost based machine to give most prominent advantage [12].

A broad open cloud will consolidate various center points and the centers in different area regions. Cloud distributing used to manage this broad cloud. A cloud package is a subarea of general society cloud with divisions considering the geographic zones [13]. In cloud master we can see three special counts. Round Robin is an unpredictable assessing based figuring. It infers it picks the load indiscriminately if that some server is strongly stacked or some are delicately stacked. Likewise spread current execution count process handle with necessities. It proper the store aimlessly by checking the size and trade the pile to that virtual machine which is daintily stacked or handle that endeavor straightforward and take less time, and give enhance throughput. It is spread achieve structure in which the heap balancer spread the heap of the occupation close by into different virtual machines. Throttled estimation is totally in context of virtual machine. In this customer first asking for the stack balancer to check the advantage virtual machine which get to that store effectively and perform the operations which is given by the customer or client. In this figuring the customer first demands the heap balancer to locate a suitable Virtual Machine to perform the required operation.

## 3. PROPOSED SYSTEM ARCHITECTURE

The proposed system model consists of the following parts: Client Login and verify code, Prefetching Data and Piggyback Information and Client Access I/O. It is given in the Figure-1.

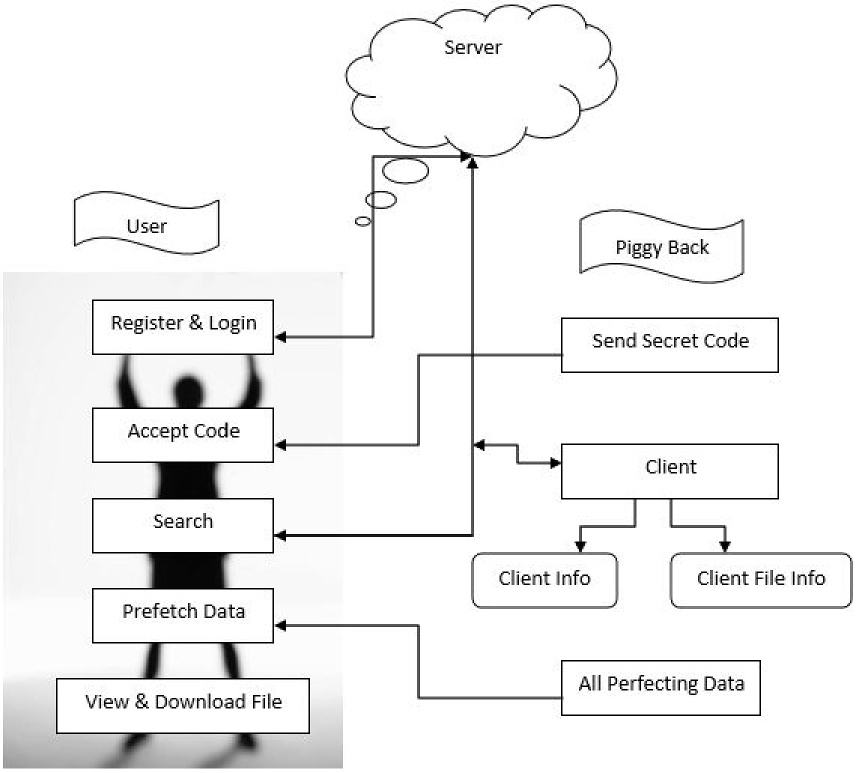


**Figure-1.** Proposed system model.

### 3.1. Client login and verify code

At first users has to register themselves with the necessary details. After the registration the client has to be login with their user id. Now the user can give request to the server and the response will be received by the user. User must verify secret code and access next server side data distribute our client files receive from piggyback server code.

### 3.2. Prefetching data and Piggyback information

The indicated development prefetching approach the information is prefetched by farthest point servers in the wake of investigating circle I/O takes after and the information is then proactively pushed to the fitting customer file structure for fulfilling potential applications demands. The cutoff servers it is basic to get a handle on the data about customer file structures and applications. The piggybacking structure exchange related data from the customer focus point to farthest point servers for adding to indicating plate I/O access tests and sending the prefetched information. Client sending an anticipated I/O asking for as far as possible server the customer file framework piggybacks data about the customer file structures and the application. The breaking point servers can record circle I/O occasions with related customer data which anticipate that a key part will portray get to arranges and picking the destination customer file framework for the prefetched information. The customer data is piggybacked as far as possible servers so that the point of confinement servers are conceivable to record the plate I/O operations running with the data about corresponded sagacious I/O occasions. The data about clear get to circuits focus point data file descriptor change and asked for size. The data about the apropos physical access contains limit server ID stripe ID square ID and asked for size. One of the said systems game plans to control foreseeing physical access by strategy for taking a gander at plate I/O takes after the two neighbor I/O operations in the harsh circle take after won't not have any reliance.

### 3.3. Piggybacking I/O

The I/O operation fit in with a progressive stream or an unpredictable stream affirm “that the working set size on the picked structures is little appeared differently in relation to the total stockpiling measure however the size presentations noteworthy variability”. “This working set count keeps a working set (W(t, T)) time t as the game plan of access areas referenced within the strategy time break (t-T, t)". The computation will break down the working set size an edge to demonstrate whether a passageway plan change happened.

### a) Linear regression prediction

The future access events just if the progression of current access events takes after a direct get the opportunity to outline. That is to say confirming the present access plan is progressive or not is fundamental to desire precision. Another access demand comes at time Tcur beginning at location Addrcur and with a solicitation size Sizecur and solicitation Access (Addrnew, Sizenew, Tnew). The square get to history to find all piece access occasions that happened as of late after a given time point. On the off chance that the aggregate number of discovered access occasions is more noteworthy than our pre-defined limit esteem. The rate of this consecutive get to example to the rate of (Dataamount/Timeused) and Timeused is the time expended for finishing all pertinent access demands amid this period. Tserving is the time required for preparing the as of now got read ask for that the following read solicitation can be taken care of just if this got one has been fulfilled.

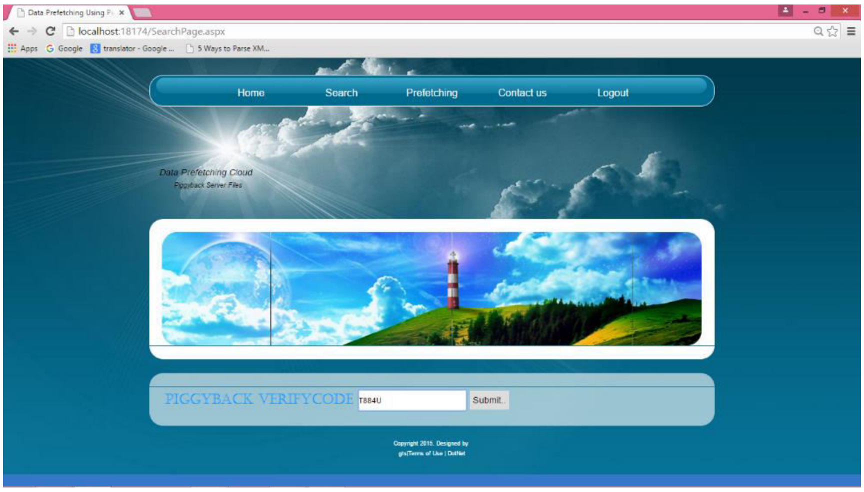
### b) Chaotic time series prediction

I/O gets to an arbitrary pattern numerous expectation "as the relationship between I/O operations is influenced by a few variables including system activity and application practices". The counterbalances having a place with "neighbor I/O operations in a stage space with an underlying detachment δZ0 wander, and after that after t cycles". I/O access expectation and comparing information prefetching ought not to be done while the entrance example is irregular however not disorderly. In a turbulent time arrangement expectation calculation to figure future I/O access. There ascertain the Lyapunov type which is a standard to show a turbulent arrangement; and foresee the future I/O access by utilizing the acquired Lyapunov type.

## 4. EXPERIMENTAL RESULTS

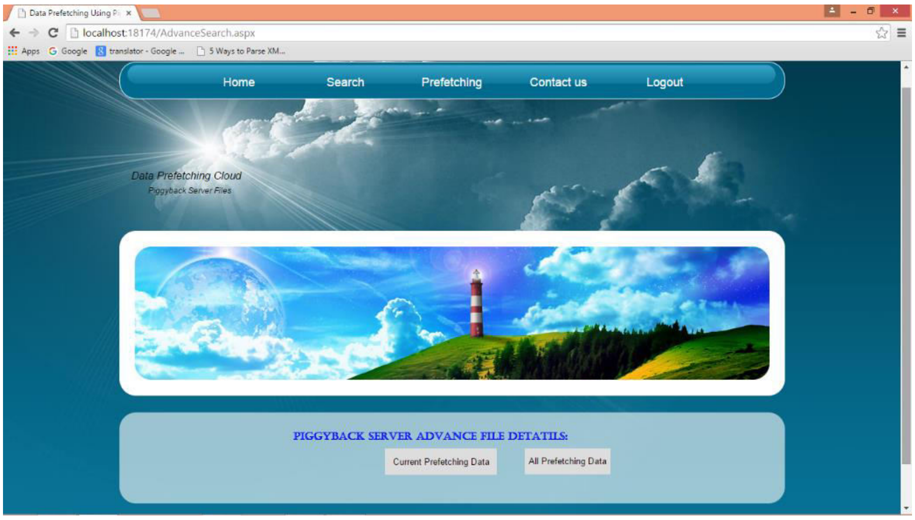
The following screenshots shows the experimental results about our proposed work.

Then the following screenshot shows the verification of the secret code.



PIGGYBACK VERIFYCODE T884U

The following screenshot shows the Advance Prefetch Data,



PIGGYBACK SERVER ADVANCE FILE DETAILS:

## 5. CONCLUSIONS

In this paper, we delineated the issue of data security in cloud data stockpiling, which is fundamentally a focal concern. With a particular finished objective to ensure the rightness of data in cloud data stockpiling, we proposed a reasonable and flexible prefetched arrangement. By guaranteeing the mystery of the data, the security of the data is envisioned. Along these lines gives the strategy all the more effective. The information stockpiling and its security in Cloud Computing requests parcel more difficulties to the clients and the suppliers. So it turns out to be more critical in the privacy of the information. The difficulties to secure the information give parcel more introductions and headings with imaginative extensions for future exploration. We imagine a few conceivable bearings for future examination on this territory.

## REFERENCES

[1] Kamara and K. Lauter. 2010. Cryptographic cloud storage. In: Proceedings of the 14th international conference on Financial cryptography and data security, ser. FC’10. Berlin, Heidelberg: Springer-Verlag. pp. 136-149.

[2] Chow. R, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85-90.

[3] Krishna P.N. Puttaswamy, *et al.* 2011. Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications. SOCC.

[4] Tribhuwan, M. R., V. A. Bhuyar and Shabana Pirzade. 2010. Ensuring data storage security in cloud computing through two-way handshake based on token management. Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on. IEEE.

[5] Sato Kanai Atsushi and Tanimoto Shigeaki. 2011. Building a security aware cloud by extending internal control to cloud. Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on. IEEE.

[6] Seung-Hyun Seo, *et al.* 2013. An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds. IEEE.

[7] Jeong-Min do. 2011. Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments. IEEE.

[8] Shridhar G.Damanal and G. Ram Mahana Reddy. 2014. Optimal Load Balancing In Cloud Computing By Efficient Utilization of Virtual Machines. IEEE.

[9] Shridhar G. Domanal and G. Ram Mohana Reddy. 2013. Load Balancing In Cloud Computing Using Modified Throttled Algorithm. IEEE International Conference. Ccem 2013. In Press.

[10] Brototi Mondal, Kousik Dasgupta and Paramartha Dutta. 2012. Load Balancing In Cloud Computing Using Stochastic Hill Climbing-A Soft Computing Approach. In Procedia Te Chnology. 4(2012): 783-789, Elsevier C3it-2012.

[11] Cao. Q, B. Wei and W. M. Gong. 2009. An Optimized Algorithm For Task Scheduling Based On Activity Based Costing In Cloud Computing. In International Conference on Esciences. pp. 1-3.

[12] Monika Choudhary, Sateesh Kumar. 2012. A Dynamic Optimization Algorithm for Task Scheduling In Cloud Environment. Peddoju International Journal of Engineering Research and Applications (Ijera). pp. 2564-2568.

[13] Gaochao Xu, Junjie Pang and Xiaodong Fu. 2013. A Load Balancing Model Based On Cloud Partitioning For The Public Cloud. Tsinghua Science and Technology Issnl L1007-0214l L04/12l Lpp34-39, 18(1).