ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

An Efficient Data Replication on Cloud Computing using MBFD with Mutual Information

Supriya Kumari, Prof.Shradha Pandit

M.Tech Student, Dept. of Computer Science & Engineering, IES College of Technology, Bhopal, India

HOD, Dept. of Computer Science & Engineering, IES College of Technology, Bhopal, India

ABSTRACT: Cloud Computing enables Scalable Computing and Storage resources. A large data-intensive applications are developed in this computing environment. Different applications have different requirements of quality-of-service (QoS). The proposed methodology implemented here for the Data Replication over Cloud Computing provides efficient Replication for Data-Intensive Applications. The proposed methodology implemented here is based on the concept of Modified Best Fit Algorithm with Mutual Information., Hence the algorithm provides efficient Execution time and average recovery time and better replication cost.

KEYWORDS: MBFD- Modified Best Fit Decreasing Algorithm; Workload in BidDataBench; Trusted Computing Group, SLA- Service Level Agreement, LQM- Layered Queuing network performance Model

I. INTRODUCTION

The recent upgradations in technology has changed the way how electronic data is stored and retrieved. Nowadays, entities and initiatives are progressively utilizing remote facilities (such as Dropbox [1], Google Cloud Stowage [2] and Amazon Humble Storing Service [3]), mainly for economical benefits. These facilities not only document material allocation but also guarantee obtainability of data from anywhere at any time. However, the use of remote services raises serious privacy issues by putting personal data at risk, particularly when the server's offering such services are untrusted. For defensive statistics from servers in untrusted surroundings, data should be encrypted before leaving trusted boundaries. Regardless of whether the data is encrypted or not, the server have to decide who will increase admittance to it. For regulating access to the data, access regulator strategies could be specified. These are admittance regulator strategies that will describe who can gain access to the data. State-of-the-art policy-based systems can ensure application of these policies. However, the substance develops difficult when delicate strategies, which may leak isolated material, have to be compulsory in untrusted surroundings. Though everywhere may steady be some misunderstanding as to what precisely Cloud Computing earnings, and no overall agreement on a definition for Cloud Figuring has remained reached [4, 5], for the possibility of these work we will accept the casual definition of Cloud Computing planned in [6] and testified under:

Cloud Totaling is a perfect for allowing appropriate, on entitlement grid admittance to a collective puddle of configurable totaling properties (e.g., networks, servers, storage, applications, and amenities) that can be speedily provisioned and unobstructed with insignificant society exertion or provision provider interaction.

Cloud Computing is the enhance technology where we can get platform as a service(PaaS), software as a service(SaaS) and infrastructure as a service(IaaS). Once it originates to storing as a facility, data privacy and data utilization are the primary issues to be dealt with. To handle the transaction of files to and from the cloud waitperson, the archives are encrypted before being subcontracted to the profitable public mist. Cloud calculating is an emergent model offering outsourced services to enterprises for storing and processing a huge amount of data at very competitive costs. However, they do not sustenance admittance regulator strategies to normalize admittance to a certain subgroup of the deposited statistics. State-of-the-art policy based mechanisms can effort only once they are organized and functioned within an important sphere [7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

There exist explanation in security concerns and research for its effectiveness but nobody of them focuses on the both problems simultaneously.
In cloud computing, one of the strong obstacles of the cloud is to preserve confidentiality of the data [8]. There are several techniques that can guarantee confidentiality of data stowed in subcontracted settings while supporting basic search capabilities [9–10]. In an untrusted environment, access policies may disclose evidence about the statistics they purpose to defend.
To understand how access policies may disclose delicate evidence in outsourced environments, let us imagine a situation where a healthcare provider has outsourced its health record management services to a third party service provider.
The fundamental notion of cloud computing is the separation of applications from the operating systems and the hardware on which they run. Cloud computing convey applications via the internet, which are accessible from net browsers and desktop and movable apps, however the software, statistics are stored on servers at an isolated position.
Today, our statistics is wandering yonder the limitations of our individual computers and all our statistics would still safely exist in on the web, available from any Internet-connected computer, anywhere in the ecosphere since of cloud computing.

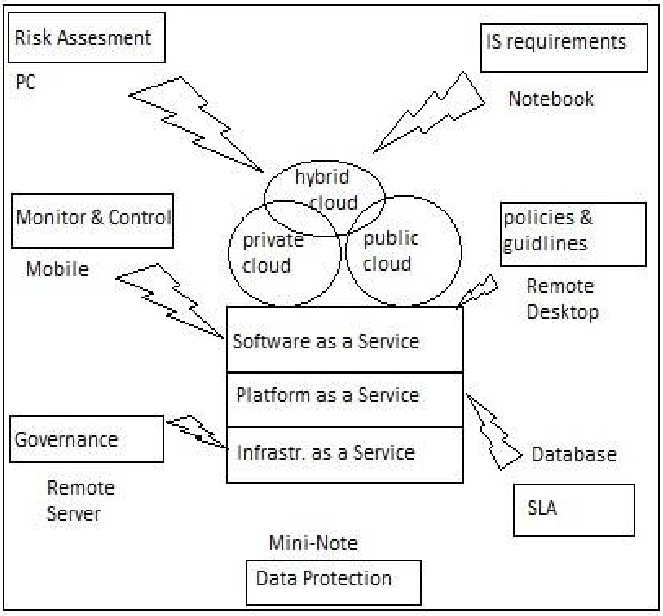

Figure : Cloud Computing

Cloud makes it possible for operators to usage amenities delivered by haze earners from anywhere at any time. The high development in virtualization and cloud calculating skills imitate the quantity of occupations that are increasing nowadays, necessitate the amenities of the simulated engine. Dissimilar types of occupation preparation processes have been practical on dissimilar types of statistics assignments. Where results are measured with different performance parameters to evaluate the performance. Ob-scheduling algorithms are developed to accomplish several areas like probable consequence, effectual use of possessions, low makespan, high quantity, better superiority of package, keeping effectiveness. In job scheduling algorithms, priority of jobs is a challenging issue since some works need to be serviced first than those other jobs which can vacation for an extended period. Appropriate job development procedure must reflect the importance of a job [11]. Figure shows the essential characteristics of cloud computing such as resource combining, wide-ranging system admittance, springiness, on-demand amenities, corporeal cloud capitals(Organization Near) and middleware aptitudes form the root earner of transporting IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) in the form of a collection of transparently data centers, runtime environment and composition tools which condolance the making, placement and implementation process of application in the cloud. Finally, to provide the above mentioned services, positions of replications such as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Community Mist, Secluded Cloud, Cross Cloud and Public Cloud are used by the mist earners. The infrastructure of the cloud is provided publicly, so that anyone can access services from anywhere publicly. Whereas, isolated cloud is used for a solitary group only. Previous cloud is Mixture Cloud, that is a cloud formed by the composition of two or more clouds that is private, community, or public [12].

SLA (Service-Level Agreement) plans all features of cloud facility practice and the response abilities of both provision breadwinners and customers, counting numerous performance descriptors together mentioned to as QoS, which may include response time, obtainability, quantity, dependability, safety, and many others. An important subset of performance indicators, which this work deals with, consists of response time, task blocking probability, probability of immediate service, and mean quantity of errands in the scheme.

To the best of our knowledge, current Cloud technology is not completely custom-made to manage QoS requirements and to admiration probable SLAs, though both the manufacturing and the educational investigation communities are presented mounting attention on issues of QoS affirmation within the context of Cloud Computing. In universal, reverence an SLA necessitates an accurate calculation of the quantity(and characteristics) of the desirable capitals.

As of today, in instruction to safeguard that a submission SLA is not dishonored, a reserve abundance strategy is often accepted. We have industrialized one such architecture; some preliminary results we have obtained from our development are discussed in [13]. Here a method describe for attaining reserve optimization at track period by using presentation replicas in the expansion and placement of the requests running in the Cloud. This approach is based on a so-called Layered Queuing network performance Model (LQM, a kind of extended queuing network model) that predicts the effect of simultaneous changes (e.g., resource allocation/de-allocation) to many decision variables (throughputs mean service delays, etc.). Moreover such a model seems to take no account of variables that could heavily affect the performance of the applications hosted in the Cloud. Examples of such variables comprise:

1. imaginable bottlenecks fashioned by load balancers, records, and bids repetition;
2. the provision times required for the introduction of a new VM in the virtual pool;
3. the instance forgotten from the preface of the original VM in the practical puddle until it reaches a fixed circumstances.

Here they observe that the performance of an application hosted in a Cloud environment can be heavily affected by the existence of other virtual machines hosting other applications on a shared server. Theyproposes a Cloud optimization infrastructure structured in layers. A feedback adaptive loop based on model, estimation and prediction techniques specific to each layer allows the optimization component to take proactive steps to provision more hardware and software resources to avoid loss of revenue or users.

III. LITERATURE SURVEY

To attain a protected and trustworthy cloud storage provision, a secure multi-owner statistics distribution method is proposed according to any user in the group so that they can steadily portion statistics with others users by the un-trusted cloud. the group manager is used for decrease of the implementation time of the key cohort at the user end or statistics proprietor side. Public-key cryptosystem construct fixed-size ciphertext as essential allocation of decryption privileges for any set of ciphertexts are achievable. Anyone can deal with any set of clandestine keys and make them as squeezed as a single key. The private key proprietor can generate a fixed-size aggregate key of ciphertext set in cloud, but another encrypted files external stay behind secret. The aggregate key strongly sent to users or kept in a smart card with limited storage.

In particular, their approach is additional supple than ranked key duty which can only accept places if all important containers portion a comparable customary of rights approaches give the primary public-key enduring forbidden encryption for elastic ladder, which was until now to be known. The difficult trouble is how to efficiently share encrypted data. Obviously users can transfer the encrypted statistics from the storing, decrypt them then direct them to others for distribution, but it misplaces the worth of cloud stowage. However, finding an efficient and safe way to share unfinished data in cloud storage is not insignificant. An inadequacy of their work is the predefined bounce of the number of maximum ciphertext classes. In cloud storage, the number of ciphertextsare not produces quickly. So we have to hold back an adequate amount of ciphertext classes for the upcoming expansion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The Trusted Computing Group (TCG) provided the trusted computing technology. This differentiate knowledge is questionably the combination of ancestries of belief into processer podia. The TCG create this mechanism as its core criteria to define the technology specification.

Since the internet or network computing has the main computing from the end of the last century. The model of trusted computing is being developed to the network computing, especially the distributed systems environment.

In this paper, author presents a new privacy-preserving refuge explanation for mist services. Here in this method deal with user unspecified admission to cloud facilities and communal stowage servers using non-bilinear group signatures to ensure anonymous authentication of cloud service client's user. Users use interfere resilient strategies during the cohort and stowage of user keys to defend beside conspiracy doses. This signifies that user's personal attributes (age, valid registration, fruitful imbursement) can be established without make knowing user's identity. Consequently, users can use services without any threat of profiling their performance. On the other hand, if users break provider's rules, their access rights will be withdrawn. Here we analyze modern privacy preservative explanations for cloud facilities and summarize our explanation based on progressive cryptographic machineries it also offers unidentified admission, unlink aptitude and the confidentiality of communicated statistics. Due to this fact, cloud provision earners using our solution can authenticate more clients in the same time. This method also provides the experimental results and measures up to the performance with related solutions.

In this paper author has try to assess how can cloud providers earn their customer's trust and provide the security, reliability and privacy when a third party used sensitive data in a remote machine established in various countries. An utility cloud has been characterized to provide a variety of services to the users. Various technologies can help to focus on security, privacy and trust challenges in cloud computing. Unlikely, the implementation of cloud computing came before the suitable technologies become visible to deal with the supplementary confronts of trust. This opening between implementation and improvement is so extensive that cloud computing clients don't fully expect this innovative way of computing. To close this opening, we require identifying with the trust issues join together with cloud computing from both a technology and business perception. Then we'll be able to establish coming up technologies that could best address these problems.

Here the author has analyzed the important features in the cloud calculating situation and the function of trusted computing platform in cloud computing. The advantages of this move toward are to make a large trusted computing technology into the cloud computing environment to accomplished the trusted computing prerequisites for the cloud computing and then accomplished the trusted cloud computing. The importance of trust varies from organization to organization, depending on the data's value. Additionally, the less expectation an endeavor has in the cloud provider, the more it wants to be in charge of its data smooth the technology. On the other hand, it's fundamental that consumers and providers change their way of thinking's. Trusting cloud computing might differ from trusting other systems, but the objective stay behinds the same to improve business and continue aggressive by take advantages of the advantages of a new technology. Any new technology must progressively build its standing for good presentation and security, earning user's trust over time. We will make more protocol to make available high security for security management, Business continuity management, Identity & access management, Privacy & data protection and application Integrity in the future.

In this arrangements can be real-world on highest of any DPDP procedure where the customer has no secret key, as distinct by Erway et al.. Here their arrangements are the only approaches that can be used for authorized negotiation not public verifiability of any DPDP scheme, to the best of our knowledge. Flowingly, in the performance subdivision, here they only compare two of our methods. Here they provided the first constructions of general-purpose negotiation methods that are appropriate to various static and dynamic circumstances, and proficient of performing fully-automated settlement by a Judge. Here their model builds upon the DPDP model , and thus is applicable to a wide range of protocols. We believe, the adding together of our method on top of DPDP protocols may to a great extent improve the use of secure cloud storage in enterprise settings, since now the client and the server may determine their difference of opinions with authorization at a persuade, paying very low computation and communication simplicity.

In this paper, we present such a system—Cloud Capacity Manager (CCM)—an on-demand calculate capacity organization and its methods for dynamically multiplexing the compute capacity of virtualized data centers at scales of that combines various low-overhead techniques, motivated by practical on-field observations, to achieve scalable capacity allocation for thousands of machines. CCM achieves this capacity by using three-level hierarchical management architecture. CCM also focus on the adjustments due to two inescapable matters in large-scale commodity data centers:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

1) preserving low working overhead, given variable cost of accomplish organization processes important to apportion capitals, and 2) managing with the augmented occurrences of these operations' failures.
In this paper, for the leading time, we describe and analyse the stimulating problem of privacy-preserving multiple keyword hierarchical exploration over encoded cloud statistics (MRSE), and found a set of severe privacy for such a secured cloud data operation organization to developed a reality.
This paper aims to provide search a file over cloud environment using multiple keywords representing the file with various predictable situations. The aim is to deliver the safety to its maximum range by including encryption and decryption methods. Approval of the users by the administrators permitted the files involved to transfer more safely. Encryption and decryption of both file name which uses asymmetric and symmetric key algorithms respectively. The secret key is generated for every user to protect any other user to misuse the file. The data that are stored in the cloud has to be protected from any attack that is caused both by external and internal attackers. Most of the interior contest are used by the cloud providers by using same relevance and analyzing the statistical leakage. Based on the usage of the file over ranked manner, it is easy to get all the details of the most used files through probability prediction. This kind of data leakage should be completely avoided and maximum protection to the data is given. The solution suggests the same by applying some new concepts to increase the data security.

IV. PROPOSED ALGORITHM

The Proposed Methodology implemented here contains of following steps to be performed for any type of Workload in BigDataBench.
1. First of all select BigDataBench Workloads with the following set of assumptions such as a) Paying equal attention to different types of applications: online service, real-time analytics, and offline analytics; b) Covering workloads in various and representative application scenarios; c) Including different data sources: text, graph, and table data; d) Covering the representative big data software stacks.
2. Selection of Different Workloads including Wordcount, Scan, Sort, Read, PageRank, Index.
3. On the basis of Different Workloads such as Wordcount Semantic Similarity using Cosine Similarity is computed and hence applying Resource Allocation using MBFD is done.

Cloud consumers can submit their requests for the access of resources to the brokers. Each of the requests from the cloudlets is allocated to their respective brokers who can process their requests.
Virtual machines can be dynamically started and stopped on a single physical machine according to the incoming requests, hence providing the flexibility of configuring different portion of resources on the same physical machine to different requirements of service requests. Multiple VMs can simultaneously run applications based on different operating system environments on a single physical machine. By dynamically migrating VMs across physical machines, workloads can be consolidated and unused resources can be switched to a low-power mode, turned off or configured to operate at low-performance levels in order to save energy.
The underlying physical computing servers provide the hardware infrastructure for creating virtualized resources to meet service demands.
Currently, resource allocation in a Cloud data center aims to provide high performance while meeting SLAs, without focusing on allocating VMs to decrease energy consumption. To increase both performance and energy efficiency, three crucial issues must be addressed. First, excessive power cycling of a server could reduce its reliability. Second, turning resources off in a dynamic environment is risky from the QoS perspective. Due to the variability of the workload and aggressive consolidation, some VMs may not obtain necessary resources under peak load, and fail to meet the desired QoS. Third, ensuring SLAs brings challenges to accurate application performance management in virtualized environments. All these issues requires effective consolidation policies that can decrease energy consumption without compromising the user-specified QoS requirements.

Allocation of Virtual Machines
Here the allocation of virtual machines is based on the arrival of new requests for the provisioning of Virtual Machines and then allocation of these virtual machine on hosts and then optimization of the current allocation of virtual machines. The proposed algorithm implemented here uses Bin backing algorithm which is based on Modified Best Fit

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Decreasing (MBFD) algorithm in which sort of all VMs in decreasing order of their current CPU utilizations, and allocate every VM to a host that provides the less increase of power consumption. This allows prestige the diversity of resources by choosing the most power-efficient nodes first.

Algorithm: Modified Best Fit Decreasing (MBFD)
Input: HostList&VMList
Output: Allocation of VM's

1. First of all sort the list of virtual machine lists in decreasing order of their Utilization.
2. For each of the Virtual machine repeat
3. manpower ← MAX
4. allocatedHost← NULL
5. for each of the host in HostList do
6. if host has enough resource for VM then
7. power ←estimatePower(host,VM)
8. if power < manpower then
9. allocatedHost← host
10. manpower ← Power
11. if allocatedHost≠ NULL then
12. allocated VM to allocatedHost
13. return allocation

- **Data content similarity (SimC)**

It is the Cosine similarity between the term frequency vectors of d1 and d2:

$$\boldsymbol{SimC(d1,d2)} = \frac{\boldsymbol{V_{d1} * V_{d2}}}{\left\|\boldsymbol{V_{d_1}}\right\| * \left\|\boldsymbol{V_{d_2}}\right\|} \qquad (1)$$

Where Vd is the frequency vector of the terms inside data unit d, ||Vd|| is the length of Vd, and the numerator is the inner product of two vectors.

- **Number of Common Neighbors**

It is defined as the total number of nodes that are connected directly in relationship with node p and q for unweighted network,

$$CN(p,q) = \varphi(p) \cap \varphi(q) \qquad (2)$$

Where, $\varphi(p)$is the set of neighbors of node p.

$\varphi(q)$is the set of neighbors of node q.

To calculate link prediction between nodes for unweighted network common neighbors can be calculated as,

$$CN(p,q) = \sum_{r\in\varphi(p)\cap\varphi(q)} w(p,r) + w(q,r) \qquad (3)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

- **Jaccard Coefficient**

It is defined as the highest proportion of common neighbors to the total number of neighbors in the network. The Jaccard Coefficient can also defined for weighted as well for unweighted network.

For unweighted network,

$$JC(p,q) = \frac{\varphi(p) \cap \varphi(q)}{\varphi(p) \cup \varphi(q)} \qquad (4)$$

For weighted network,

$$JC(p,q) = \sum_{r \in \varphi(p) \cap \varphi(q)} \frac{w(p,r) + w(q,r)}{\sum_{a \in \varphi(p)} w(a,p) + \sum_{b \in \varphi(q)} w(b,q)} \qquad (4.5)$$

Predict the most valuable words from the text documents having most similarity between words.

Skewness algorithm for the avoidance of overload

Here Skewness algorithm is applied for the avoidance of the overload by applying the predicting the unevenness in the allocations of resources. The 'N' number of resources allocation with 'R' number of resources can be applied to their respective servers P on the basis of:

$$skewness(P) = \sqrt{\sum_{i=1}^{n} (\frac{r_i}{\bar{r}})^2}$$

Where, $\bar{r}$ is the average utilization of all the resources for the'N' number of resources for Servers P. Finallly the mitigation of resource can be done by comparing the threshold. The Utilization for each of the resource can be allocated on the basis of load on each of the server.

PROPOSED ALGORITHM

1. Create homogenous and heterogeneous cloud environment for public, private and hybrid clouds.
2. Establish and initialize datacenters and V.M's and cloudlets and brokers to access the data to the data centers from users.
3. Send all requests 1st time.
4. If 'Pkt' be the packets to be send from sender to broker for the access of 'N' resources R1,R2,R3…..Rn
5. The transport power to access the resource Ri is given by

$$P_{T,IP} = 2.H.P_{tr1} + (H-1).P_{IP}$$

Where, H is the number of users to send the request for the resource Ri and P_{tr1}, P_{IP} represents power of consumption for the resource Ri and processing cost.

6. Find the dirty requests to be sent in next iteration using 2 phase algo.
7. Find the zero pages in requests
8. If request is zero page,

   Send 1 byte only "no data"

9. Apply the hash similarity function to identify the similar and identical requests
10. And more than one identical request are there then send only one.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

1. If 'N' of request are send from User 'Ui' to DataCenter 'Di'
2. If 'Ri' is the resources to be involved in the communication.
3. For each of 'Ri' → 'Di'
4. Compute power for each of the resource
   $P_{T,IP} = 2.H.P_{tr1} + (H-1).P_{IP}$
5. If check 'Rold'==Rnew' request for new resource and new resource is same or not.
6. Send only 'Rold'
7. Else
8. Send Rnew
9. End

Resource Scheduling Technique

While(true){
Tcurrent = get Raccess from VM;
for each Resource{
//resource is unallocated
If (!Tcurrent[Resource])
For each Useri→ Resource
Allot Useri→Tcurrent
Else
WaitT→ till Resource(Alloted)
End
End

V. RESULT ANALYSIS

The table and figure shown below are the analysis and comparison of Total replication cost between existing and proposed work. The Proposed Work implemented here provides efficient Replication cost in comparison with existing work.

	Total Replication Cost (S)	
# of Requested Nodes	Existing Work	Proposed Work
500	1000	900
1000	9000	8000
1500	15000	14000
2000	20000	19000
2500	25000	24000

Table 1. Analysis of Total Replication Cost

The figure shown below is the analysis and comparison of Total replication cost between existing and proposed work. The Proposed Work implemented here provides efficient Replication cost in comparison with existing work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

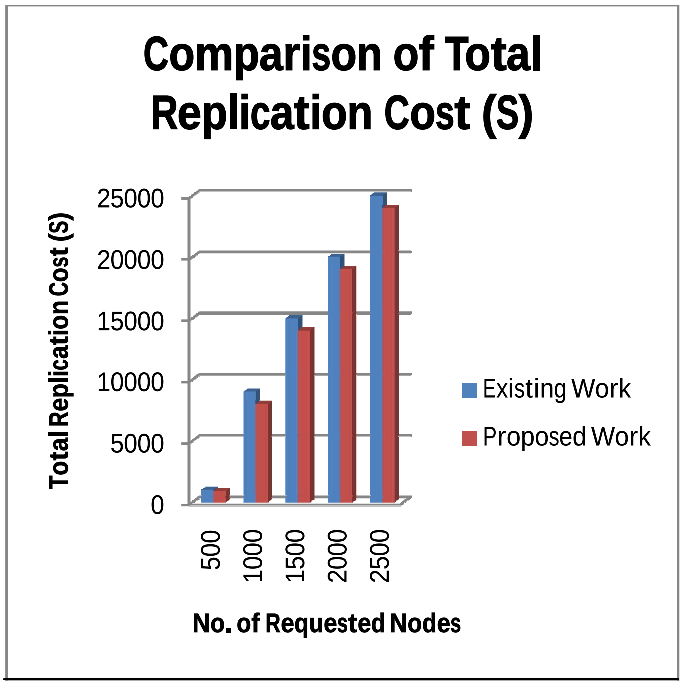

Figure 1.Comparision of Total Replication Cost

The table shown below is the analysis and comparison of Average Recovery Time between existing and proposed work. The Proposed Work implemented here provides efficient Recovery Time in comparison with existing work.

	Average Recovery Time (S)	
# of Requested Nodes	Existing Work	Proposed Work
500	4	3.4
1000	4.2	3.8
1500	5	4.3
2000	5.5	5.1
2500	5.7	5.3

Table 2. Analysis of Average Recovery Time

The figure shown below is the analysis and comparison of Average Recovery Time between existing and proposed work. The Proposed Work implemented here provides efficient Recovery Time in comparison with existing work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

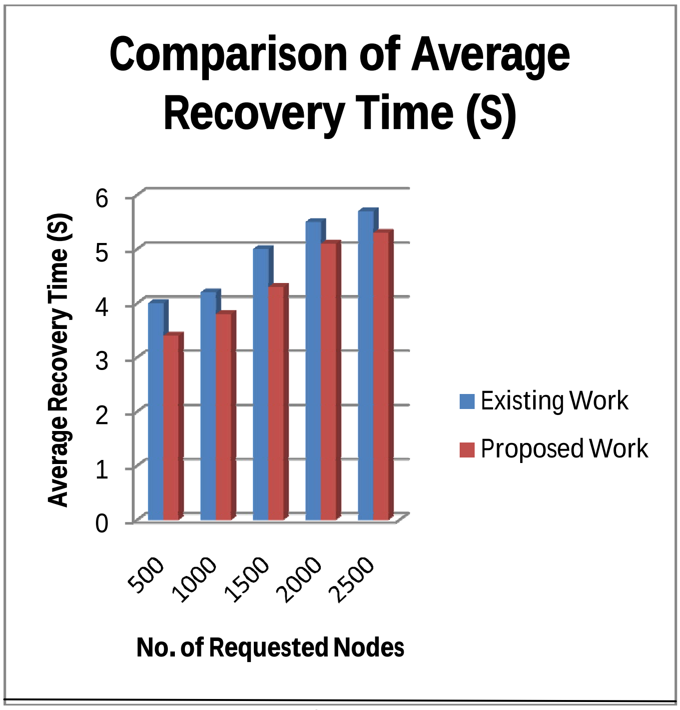

Figure 2. Analysis of Average Recovery Time

The table shown below is the analysis and comparison of Execution Time between existing and proposed work. The Proposed Work implemented here provides efficient Execution Time in comparison with existing work.

	Execution Time (S)		
# of Requested Nodes	Existing Work	Proposed Work	
500	1.3	1.1	
1000	3	2.8	
1500	4.2	3.6	
2000	4.9	4.3	
2500	5.1	4.8	

Table 3. Analysis of Execution Time

The Figure shown below is the analysis and comparison of Execution Time between existing and proposed work. The Proposed Work implemented here provides efficient Execution Time in comparison with existing work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

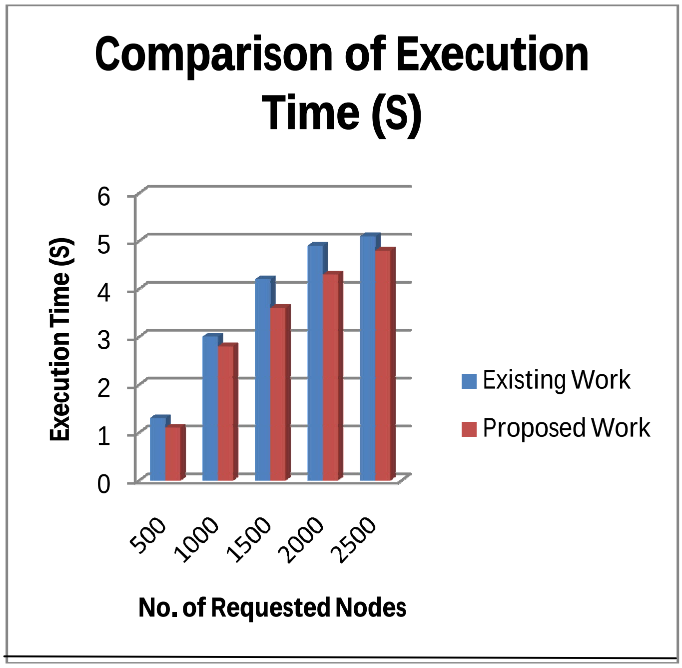

Figure 3. Analysis of Execution Time

VI. Conclusion and Future Work

The proposed methodology implemented here for the Data Replication over Cloud Computing provides efficient Replication for Data-Intensive Applications. The proposed methodology implemented here is based on the concept of Modified Best Fit Decreasing (MBFD) Algorithm with Mutual Information., Hence the algorithm provides efficient Execution time, average Recovery time and better Replication cost

References

[1] "Dropbox." https://www.dropbox.com/ . October 30, 2013.
[2] Google, "Google cloud storage pricing." https://cloud.google.com/pricing/cloud-storage, February 2013.
[3] Amazon, "Amazon simple storage service (Amazon S3)." http://aws.amazon.com/s3/#pricing, February 2013.
[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53:50–58, April 2010.
[5] Q. Zhang, L. Cheng, and R. Boutaba.Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1:7–18, 2010. 10.1007/s13174-010-0007-6.
[6] P. Mell and T. Grance.The NIST Definition of Cloud Computing (Draft)–Recommendations of the National Institute of Standards and Technology.Special publication 800-145 (draft), Gaithersburg (MD), Jan. 2011.
[7] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," Computer, vol. 29, no. 2, pp. 38–47, 1996.
[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, pp. 50–58, Apr. 2010.
9] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidimensional range queries over outsourced data," The VLDB Journal, vol. 21, no. 3, pp. 333–358, 2012.
[10] Y. Yang, F. Bao, X. Ding, and R. H. Deng, "Multiuser private queries over encrypted databases," Int. J. Appl. Cryptol., vol. 1, pp. 309–319, Aug. 2009.
[11] Ghanbari, Shamsollah, and Mohamed Othman. "A Priority based Job Scheduling Algorithm in Cloud Computing." Procedia Engineering 50 (2012): 778-785.
[12] R.Madhubala, "An Illustrative Study on cloud computing", "International Journal of Soft Computing and Engineering", Vol.1, issue.6, January 2012, pp. 286-290.
[13] Chona S. Guiang, Kent F. Milfeld, AvijitPurkayastha, and John R. Boisseau. Memory performance of dual-processor nodes: comparison of intelxeon and amdopteron memory subsystem architectures. In Proceedings for ClusterWorld Conference and Expo 2003.