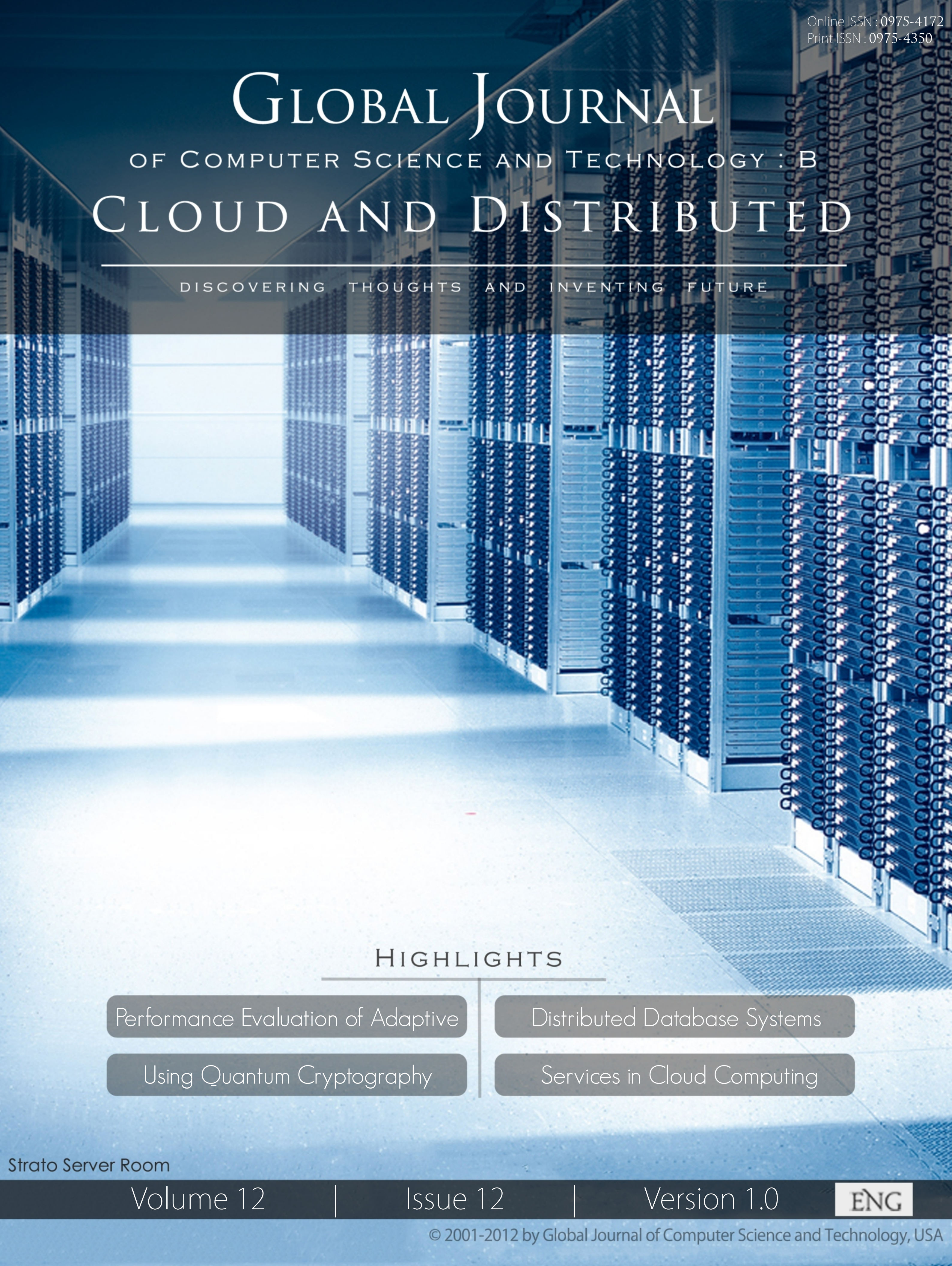
Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology : B

Cloud and Distributed

DISCOVERING THOUGHTS AND INVENTING FUTURE



Highlights

Performance Evaluation of Adaptive

Using Quantum Cryptography

Distributed Database Systems

Services in Cloud Computing

Strato Server Room

Volume 12 | Issue 12 | Version 1.0

ENG

Global Journal of Computer Science and Technology: B
Cloud & Distributed

Global Journal of Computer Science and Technology: B
Cloud & Distributed

Volume 12 Issue 12 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Global Association of Research
Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141
United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU
United Kingdom.

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Editorial Board Members (HON.)

Contents of the Volume

Global Journal of Computer Science and Technology
Cloud & Distributed
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation of Adaptive Scheduling Algorithm for Shared Heterogeneous Cluster Systems

By Amit Chhabra & Gurvinder Singh
Guru Nanak Dev University, Amritsar, India

Abstract - Cluster computing systems have recently generated enormous interest for providing easily scalable and cost-effective parallel computing solution for processing large-scale applications. Various adaptive space-sharing scheduling algorithms have been proposed to improve the performance of dedicated and homogeneous clusters. But commodity clusters are naturally non-dedicated and tend to be heterogeneous over the time as cluster hardware is usually upgraded and new fast machines are also added to improve cluster performance. The existing adaptive policies for dedicated homogeneous and heterogeneous parallel systems are not suitable for such conditions. Most of the existing adaptive policies assume a priori knowledge of certain job characteristics to take scheduling decisions. However such information is not readily available without incurring great cost. This paper fills these gaps by designing robust and effective space-sharing scheduling algorithm for non-dedicated heterogeneous cluster systems, assuming no job characteristics to reduce mean job response time. Evaluation results show that the proposed algorithm provide substantial improvement over existing algorithms at moderate to high system utilizations.

Keywords : adaptive space-sharing scheduling, cluster computing systems, non-dedicated heterogeneous clusters, performance evaluation and mean response time.

GJCST-B Classification: C.1.4

PERFORMANCE EVALUATION OF ADAPTIVE SCHEDULING ALGORITHM FOR SHARED HETEROGENEOUS CLUSTER SYSTEMS

Strictly as per the compliance and regulations of:

OPEN ASSOCIATION OF RESEARCH SOCIETY, USA
RESEARCH | DIVERSITY | ETHICS

Performance Evaluation of Adaptive Scheduling Algorithm for Shared Heterogeneous Cluster Systems

Amit Chhabra [α] & Gurvinder Singh [σ]

Abstract - Cluster computing systems have recently generated enormous interest for providing easily scalable and cost-effective parallel computing solution for processing large-scale applications. Various adaptive space-sharing scheduling algorithms have been proposed to improve the performance of dedicated and homogeneous clusters. But commodity clusters are naturally non-dedicated and tend to be heterogeneous over the time as cluster hardware is usually upgraded and new fast machines are also added to improve cluster performance. The existing adaptive policies for dedicated homogeneous and heterogeneous parallel systems are not suitable for such conditions. Most of the existing adaptive policies assume a priori knowledge of certain job characteristics to take scheduling decisions. However such information is not readily available without incurring great cost. This paper fills these gaps by designing robust and effective space-sharing scheduling algorithm for non-dedicated heterogeneous cluster systems, assuming no job characteristics to reduce mean job response time. Evaluation results show that the proposed algorithm provide substantial improvement over existing algorithms at moderate to high system utilizations.

Keywords : adaptive space-sharing scheduling, cluster computing systems, non-dedicated heterogeneous clusters, performance evaluation and mean response time.

I. Introduction

Traditionally multiprocessors were used as parallel computing platform to execute large-scale grand challenging applications. But for over the past decade, there have been unprecedented technological advances in the commodity personal computers (PCs) and network performance, mainly as a result of faster hardware and more sophisticated software. Another predominant trend witnessed during this era was the falling prices of these technologies. Both of these trends intuitively stimulated the creation of new cost-effective and high-performance networked-computing based parallel and distributed paradigm centering on the use of cluster of low-cost PCs (and/or workstations) interconnected with low-latency, high-bandwidth networks (like ATM, switched Fast or Gigabit Ethernet etc.). Clusters of PCs are becoming a commonplace high-performance computing platform in universities which enjoy the in-house availability of cluster constituents such as PCs and internetworking devices as commodity-off-the-shelf (COTS) components.

On par with the development of clusters as a parallel processing platform to execute large-scale applications (also known as jobs), scheduling on clusters has been an interesting research area to work with in recent years. Job schedulers are generally designed to resolve the contention among multiple competing jobs to acquire the available computational resources (such as processors, memory, storage etc.).

Parallel job scheduling problem is widely studied in traditional multiprocessor systems [3-6] and to a relatively less extent in cluster computing systems [1-2]. A common assumption in most of the existing parallel job scheduling research in both these systems, has been that all processors in the system have equal processing capacity (i.e., homogeneous) and dedicated. In contrast, in this paper we focus on proposing a scheduling algorithm to allocate processors to jobs in non-dedicated and heterogeneous cluster computing environment.

The rest of the paper is organized as follows: Section 2 discusses background knowledge on cluster computing systems and scheduling. Section 3 states the problem statement. Section 4 gives an overview of previous literature work related to the problem and describes the details of the proposed solution. Section 5 describes simulation model which discusses the workload and system model used. Section 6 evaluates the performance of new policies and compares them with existing solutions and Section 7 concludes the paper.

II. Background Knowledge

In recent times, paradigm of parallel processing in various organizations has been shifted from traditional expensive multiprocessors to commodity-based high-performance clusters due to their high-performance and cost-effectiveness. Clusters of PCs or workstations based on the duration and availability of amount of processing capacity can be generally classified into two

Author α : Assistant Professor in the department of computer science and engineering, Guru Nanak Dev University, Amritsar, India.
E-mail : chhabra_amit78@yahoo.com
Author σ : Professor in the department of computer science and engineering, Guru Nanak Dev University, Amritsar, India.
E-mail : gsbawa71@yahoo.com

classes; 1) High Performance Computing (HPC) systems, and 2) High Throughput Computing (HTC) systems. HPC systems are suitable for interactive parallel jobs as they deliver enormous amount of processing capacity over short periods of time. HTC systems provide large amounts of processing capacity over long periods of time and hence suitable for batch parallel jobs. Within these two classes, cluster computing systems are further classified into three categories [1-2] as follows:

1. Volunteer-owned Cluster Computing (VCC): Individual computer in the system may be homogeneous or heterogeneous and is assumed to be privately owned. The machines may be used for executing externally submitted jobs only if the owner is not using it. Therefore machines in the VCC systems are non-dedicated as these are not simultaneously available to external and local users. The VCC cluster type systems are commonly used as High throughput computing (HTC) platforms.
2. Community-owned Cluster Computing (CCC): All computing machines are shareable and may be homogeneous or heterogeneous. The CCC cluster computing systems are used both as HTC and HPC environments. A computer lab in an educational institution is a best example of CCC type of systems.
3. Privately-owned Cluster Computing (PCC): PCC is a dedicated cluster of computers or workstations, which is commonly referred to as Beowulf in the literature. This kind of setup is deliberated for use either as a dedicated HTC or as a dedicated HPC platform.

Space-sharing policies are commonly used to schedule parallel jobs in distributed-memory parallel systems such as multiprocessors as well as cluster computing systems. In space-sharing policy, parallel system of multiple processors is divided into disjoint set of processors (known as partitions) so that each partition can be assigned to a single job. In this way, number of jobs can be executed side-by-side by simultaneously providing processor partitions. The number of processors in each partition to be assigned to a job is known as partition size. The primary reason for preferring space-sharing over time-sharing for cluster systems is to avoid the cost of context switching due to frequent preemptions in time-sharing systems.

Space-sharing policies can be broadly divided into fixed, variable, adaptive and dynamic policies [3-4] based on the decision that whether the partition size once assigned to the jobs can be changed during execution time or not. In fixed policies, partition sizes are fixed by the administrator before the system actually starts operating and any modification to these partition sizes require a system reboot. Variable policies require partition sizes to be specified by the user at the time of job arrival. In adaptive policies, partition sizes are determined by the scheduler at the time of job scheduling on the basis of current system load and any available job characteristics. However partition size once assigned to a job cannot be changed during job execution. In dynamic policies, partition size of a job can be changed during its execution.

High performance applications for cluster computing systems are mostly presented as parallel jobs. A parallel job is said to consist of a set of tasks running concurrently to achieve a certain common objective. Each task runs to completion on its assigned processor. The number of tasks (and hence processors required) a certain job has is referred to as the job size.

Characteristics of on-line job streams that act as input workload to the job schedulers influence the performance of the schedulers. Parallel jobs can be classified into four types [3-4]; (i) Rigid, (ii) Moldable (iii) Evolving, and (iv) Malleable, depending upon the number of processor to be allocated at submission time or during execution. A rigid job demands a fixed number of processors at the time of submission and executes on these processors exclusively until completion. Moldable jobs can be made to execute on different number of processors based on the current system load. For example if system load is high, then few processors can be assigned to the moldable job and if system load then large number of processors can be allotted to the job. However this flexibility is only available at job start time and partition size cannot be reconfigured during execution. The processor requirements of both Evolving and Malleable jobs can be changed during execution. For evolving jobs, requirement changes are initiated by the application itself during the various phases of its execution. If the system cannot satisfy the job's demand, the job has to wait for exact processor allocation. For malleable jobs, the decision to change the number of processors is made by an external job scheduler.

III. Problem Statement

Most of existing parallel job scheduling policies especially adaptive space-sharing polices have been focused on homogeneous parallel systems such as distributed-memory multiprocessors and cluster computing systems (for example PCC or VCC systems) in which all the processors are dedicated and of equal capacity. It should be noted that scheduling polices for distributed-memory multiprocessors can be directly used in PCC systems without any modification due to similarity in architectures of both the systems. However clusters of PCs such as CCC systems tend to be heterogeneous due to the fact that over the passage of time, new fast machines are regularly added to cluster or some of the obsolete cluster hardware is replaced to improve cluster computing performance. Moreover in order to improve the utilization of computing machines, the processors in CCC systems are often shared by local users to execute local jobs (hereafter known as background workload).

The problem seems significant as the partition sizes obtained in non-dedicated heterogeneous parallel systems (e.g. CCC systems) will be different from those obtained in dedicated homogeneous systems. When we partition a dedicated homogeneous cluster (such as PCC and VCC), partition size is obtained by dividing total number of physical processors by the total number of jobs in the system. But in case of non-dedicated heterogeneous systems, partition size is calculated by dividing the total available computing power of all processors by the number of jobs currently available in the system. However total available computing power will be different at different times due to variations in the computing power of individual processors in the presence of varying background workload. Hence corresponding calculated partition size changes continuously. Moreover existing adaptive policies focus on using certain job characteristics (which may not be readily and cheaply available) to calculate partition size.
Therefore an efficient adaptive scheduling policy is required which can take care of heterogeneity of processor speeds as well as run-time load variations due to background workloads executing at individual processors and above all requires no job characteristics to calculate partition size.

IV. Related Works and Proposed Algorithms

The focus of the current job scheduling research in distributed-memory parallel systems is towards adaptive algorithms to schedule moldable jobs [8-15] as they have shown to achieve better mean response time than the scheduling algorithms for rigid jobs. This is due to the fact that adaptive algorithms decide the partition sizes by adapting to current system load at job scheduling time whereas rigid jobs only require a fixed number of processors resulting into increased processor fragmentation and mean response times. Dynamic policies are shown to more suitable for shared-memory parallel systems in which the associated overheads of dynamic-partitioning are outweighed by the benefits.

Adaptive scheduling algorithms for assigning partition sizes to moldable jobs have been extensively studied in homogeneous parallel systems [5-12] and to less extent in heterogeneous parallel systems [2][13]. Existing adaptive algorithms in both homogeneous and heterogeneous cluster systems share one common assumption that processors are dedicated to execute only cluster applications (no other applications can be executed locally). Available adaptive policies also differ from each other by the amount of job characteristics used in making processor allocation decisions.

In [5-6], Rosti et al. introduced several adaptive partitioning policies (known as Fixed Processors per Job (FPPJ)), Equal Partitioning with a Maximum (EPM), Insurance Policy and Adaptive Policies (known as AP1, AP2, AP3, AP4 and AP5)) for distributed-memory multiprocessors over a wide range of workload types and with different possible arrival rates. These policies try to allocate equal-sized partitions to the waiting applications since no a priori job characteristics were assumed to be available. However these policies differ from each other in how the target partition-size is computed.

Out of these adaptive policies, AP2 (known as work-conserving policy) seems to be an interesting policy that reserves one additional partition for the future job arrivals. The partition size in the AP2 policy is calculated as shown in (1).

$$Partition\ Size\ (PS) = max\left(1, ceil\left(\frac{total\_procesors}{Waiting\_jobs+1} + 0.5\right)\right) \qquad (1)$$

In [7], Dandamudi and Yu show that AP2 considers only queued jobs to calculate partition size. This will lead to a situation that contravenes the principal of allocating equal-sized partitions to all jobs. Dandamudi and Yu, suggested a modified version of AP2 known as Modified adaptive policy (MAP) which considers waiting as well as running jobs to calculate partition size as shown in (2).

$$Partition\ Size\ (PS) = max\left(1, ceil\left(\frac{total\_processors}{Waiting\_jobs+(f*Running\_jobs)+1} + 0.5\right)\right) \qquad (2)$$

Target partition size to be finally allocated to the waiting job is calculated using equation (3). It is the minimum of the partition size calculated using equation (2) and maximum parallelism of the job.

$$Traget\ partition\ size = min(PS, maximum\ parallelism\ of\ the\ job) \qquad (3)$$

The parameter f (whose value lies between 0 and 1) is used to control the contribution of the "running" jobs to the partition size. It has been shown that the MAP policy provides significant improvement in performance over policies like AP2, ASP and ASP-max etc. that do not consider the contribution of running jobs while calculating partition size. The amount of improvement obtained is a function of parameter f, system load, and workload.

The adaptive policy proposed in [8][10] is more restrictive, in that users must specify a range of the number of processors for each job. Availability of service demand knowledge of an individual job is assumed in the paper. Schedulers will select a number which gives

Global Journal of Computer Science and Technology (B) Volume XII Issue XII Version I Year 2012

the best performance. Schedulers in [8][10] use a submit-time greedy strategy to schedule moldable jobs.

In [11], Srinivasan et al. have some improvement to [8][10]: (i) using schedule time-scheduler which defers the choice of partition size until the actual job schedule time instead of job submission time and, (ii) using aggressive backfilling instead of conservative backfilling.

In [12], Srinivasan et al. argue that an equal-sized partition strategy tends to benefit jobs with small computation size (light jobs). On the other hand, allocating processors to jobs proportional to the job computation size tends to benefit heavy jobs significantly. A compromise policy is that each job will have a partition size proportional to the square root of its computation size (Weight) as in (4). This equation is used to calculate partition size in an enhanced backfilling scheme proposed in [11].

$$WeightFraction_i = \frac{\sqrt{Weight_i}}{\sum_{i \in \{ParallelJobInSystem\}} \sqrt{Weight_i}} \qquad (4)$$

In [2], a variation of MAP, known as Heterogeneous Adaptive Policy (HAP) was suggested by Dandamudi and Zhou to work with heterogeneous parallel systems. The work introduced the concept of Basic Processor Unit (BPU) to differentiate the heterogeneous processors from each other. Partition sizes are allocated to the jobs on the basis of their computation power in terms of number of BPUs rather than using a physical processor level as in homogeneous systems. The research paper showed the supremacy of HAP over MAP and AP2 policies. Partition size in HAP is calculated as in equation (5) and target partition size is calculated using equation (3).

$$Partition\ Size\ (PS) = max\left(1, ceil\left(\frac{total\_BPUs}{Waiting\_jobs + (f * Running\_jobs) + 1} + 0.5\right)\right) \qquad (5)$$

In [13], Shim suggested various adaptive policies for shared heterogeneous network of workstations (NOW) considering the priority of sequential local jobs as well as the parallel jobs. No in-depth details about the working of the algorithms are provided in the paper and no comparisons are made with the existing policies. The shortcoming of this paper is that it considers only waiting jobs to calculate the partition size which usually lead to worse results.

In [14], Doan et al. suggested priority-based adaptive policy for homogeneous PC-based cluster systems for both rigid and moldable jobs. The user can assign priority to both types of jobs. The jobs with higher priority are given preference in execution. Since rigid jobs require the fixed number of processors (e.g. partition size), so partition-function for only moldable jobs is derived from equation (2) as given in [7].

In [15], Abawajy proposed another adaptive policy known as SOUL for heterogeneous multi-cluster systems which calculates partition size on the basis of mean service rate of heterogeneous processors, local load at processors and maximum parallelism information of waiting jobs. It has been shown that SOUL policy tends to produce shorter mean job response times as compared to both AEP and MAP at various workloads. But no comparison between HAP and SOUL policy is available.

a) Proposed Robust Heterogeneous Adaptive Policy (RHAP)

From the literature survey, following lessons have been learnt which will help us to design a robust adaptive policy for non-dedicated heterogeneous parallel systems.

1) Adaptive policies which consider both current waiting and running jobs in the parallel system perform better than those policies which consider only current waiting jobs.
2) In heterogeneous systems, BPU mechanism is used frequently to differentiate the computing power of different physical processors.
3) When no job knowledge is available, equal-sized (or equivalent) partitioning mechanism is preferred over weighted square-root fair-share strategy which requires the service demand knowledge of jobs.
4) Significant cost in terms of various overheads is involved in obtaining the a priori knowledge of various job characteristics such as maximum parallelism, average parallelism, service demand knowledge etc.

Using these observations and lessons, we have suggested few modifications to HAP policy which have shown good results over various policies in dedicated heterogeneous systems. The new policy is named as Robust Heterogeneous Adaptive Policy (RHAP) to schedule jobs in non-dedicated heterogeneous cluster environment and requires no job characteristics (as opposed to HAP) to calculate final target partition size for the current waiting jobs.

Since cluster processors can be shared between local and parallel jobs, therefore at any point of time, current available computing power for execution of parallel workload at each processor in the presence of local workload is given as in equation (6).

$$Computing\ power\ (CP_k) = BPU_k * (1 - Local\_load_k) \qquad (6)$$

In a cluster system with P processors, BPUk represents the computing power of kth processor and $Local\_load_k$ denotes the load at individual processor due to the execution of local jobs.

Ideal partition size in RHAP is then calculated on the basis of current available computing as shown in (7).

$$Partition\ Size\ (PS) = max\left(1, ceil\left(\frac{\sum_{k=1}^{p} BPU_k*(1-Local\_load_k)}{Waiting\_jobs+(f*Running\_jobs)+1} + 0.5\right)\right) \quad (7)$$

It should be noted that job scheduler is invoked only at arrival and departure time of jobs. Information about local load and computing power of each processor is also collected by the job scheduler at these times. Here "Max" is system-wide Maximum Allocation parameter which imposes an upper limit on the number of BPUs to be allocated to jobs. It is equal to some fixed percentage of the total BPUs available in the system. The number of BPUs finally allocated is calculated as follows in (8).

$$Traget\ partition\ size = min(PS, Max) \quad (8)$$

Since no knowledge about maximum parallelism of the jobs is "a priori" available to the scheduler, so there is no distinction between short and long jobs. In the absence of "Max" parameter, shorter jobs can be assigned large number of processors resulting into internal processor fragmentation and increased waiting times for other jobs. Max puts a cap on the smaller jobs that tend to retain larger partition sizes. Moreover it also avoids the situations when a long job is holding up large number of processors.

V. Simulation Model

We have implemented a discrete event simulator in .Net environment to evaluate the performance of proposed adaptive scheduling algorithms under various workload conditions. Simulation modeling is preferred over the actual experimentation as it gave us the greater flexibility of covering a wide range of application characteristics and controlled parameters like arrival rates, system utilization etc. and allowed us to abstract away trivial details of the environment under study, which otherwise would complicate the performance evaluation procedure.

The developed simulator takes the on-line job stream as input parallel workload, executes parallel workload with the specified adaptive policy and generates the output in the form of mean response time. Response time of a job is defined as the sum of its execution time and waiting time. Waiting time of job is the difference between job arrival time and job scheduling time. Execution time is the actual time spent to execute the job. It should be noted that at the time of job arrival, no job characteristics (such as number of processors required, job service demand etc.) are available to the scheduler.

a) System Model

We have used an open system model of community-owned cluster of 64 independent commodity single-processor personal computers and each computer is used in a shared mode i.e. it is able to service local sequential tasks as well as the tasks of parallel job submitted by the central job scheduler. The computers differ from each other in terms of heterogeneity in processor speeds i.e. computing power they possess. Computer and processor terms are used interchangeably in context of this paper. We assume that computers in the cluster are connected using 100Mbps Ethernet switch. Relative computing power of different physical processors is represented in terms of Basis Processing Unit (BPU) [2] which can either be derived with the help of SPECfp2000 ratings based on the processor speeds or by executing independent benchmarking programs on heterogeneous processors. We have used two types of processors in the computers of cluster system; First 32 computers contain Type I processors; Next 32 computers contain Type II processors that are twice faster than Type I processors. Hence each processor in Type I has 1 BPU and Type II processor has 2 BPUs.

b) Parallel Workload Model

Parallel workload model containing online stream of parallel jobs for scheduling contains two components; 1) job arrival process and 2) job service demand. The job arrival process is characterized by job arrival rate (λ) and coefficient of variation of inter-arrival times (CVa). High arrival rate represents that inter-arrival time between successive jobs is small. We have modeled the job arrival process using exponential distribution with CVa equal to one.

Mean service demand (D) parameter is the uncorrelated cumulative mean service demand which represents the total time required to execute the job in a dedicated environment, independent of how many processors are used. Service demand of jobs is generated using 2-stage hyper-exponential distribution with coefficient of variation of service demand (CVs) greater than one. Since moldable jobs can be made to run on the varying number of processors, therefore time (tj) taken by the parallel job varies based on the number of processors (pj) assigned to it when the job starts executing. It should be noted that dj= (tj)*(pj) as we have ignored the communication and synchronization overheads, when overall mean service demand of a parallel job (dj) is distributed equally among tasks (which are always equal to "pj" processors assigned to the job) of the job.

c) Background Workload Model

We assume abstract model for representing load due to background jobs at each processor by hiding the internal details of arrival and execution times of sequential local jobs. Each cluster processor is assumed to service a stream of background jobs that arrive at individual computers independently. *Local_load* at each processor indicates the load due to the execution of sequential local jobs. As the local load increases, computing power available to service parallel workload decreases. We model the local load using discrete uniform distribution ranging from 0% to 30% i.e. U[0%, 30%] and this information is only available to job scheduler at job arrival and departure times.

VI. Performance Evaluation and Results

In this section we will evaluate the performance of proposed algorithms in terms of mean response time and also compare the simulation results with the existing approaches. The default parameters and values used in simulation experiments are for various simulation parameters for 5000 jobs are as follows in table 1.

Table 1 : Default parameters and values used

Parameters of Parallel Jobs	Values
Mean service demand (D)	16
Coefficient of variation (CV_A) of job arrival	1
Coefficient of variation (CV_S) of service demand	4
Number of processors in the cluster	64
Max	30 % of total processing capacity

Average load or utilization of the cluster system due to parallel jobs is derived using equation (9).

$$Average\ utilization = \frac{Job\ arrival\ rate * Mean\ service\ demand}{Number\ of\ processors} \quad (9)$$

a) *Relative performance of the scheduling policies*

In this section we compare the performance of the proposed adaptive scheduling policy i.e. RHAP with the HAP and MAP policy. Since no maximum parallelism information is a priori available to the scheduler, therefore target partition size for HAP policy computed in (3) will be equal to the partition size computed in (2). The default value of 'f' in the partitioning-function for RHAP, HAP and MAP policies is set to 0.5 which is suggested as a reasonable value in existing similar research works [2][7].

RHAP policy tends to produce shorter MRT values at system loads of interest (i.e. at medium to high loads) as shown in figure 1. This is due to two reasons; 1) RHAP policy produce smaller partition sizes as compared to both HAP and MAP as it considers the background workload into account. 2) Max parameter also restricts allocation of the larger partition sizes to jobs. On the other hand, both HAP and MAP try to allocate larger partition sizes since they are not aware of any background workload. But in reality the total available computing power of all processors is much less than that of assumed by MAP and HAP. Therefore jobs have to wait for a long time to receive calculated partition sizes. HAP and MAP policies also tend to produce bigger partition sizes at low to medium system

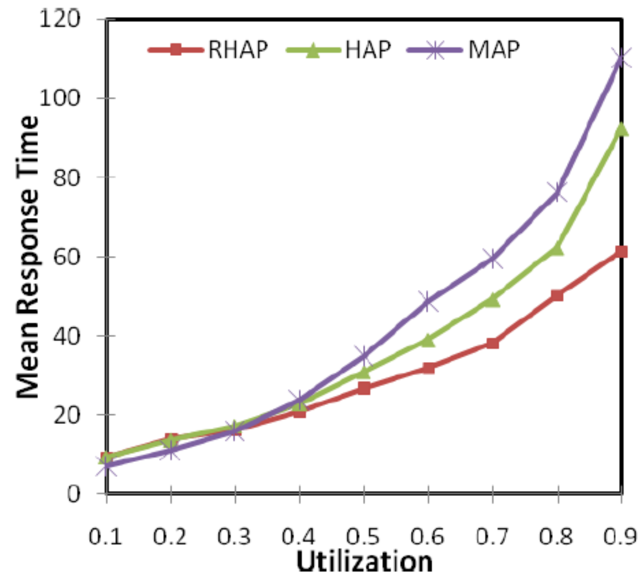


Fig. 1 : Performance of scheduling policies

Utilization since they impose no upper limit on the number of processors to be allocated to jobs. This will apparently result into allocation of large partition sizes to even smaller jobs.

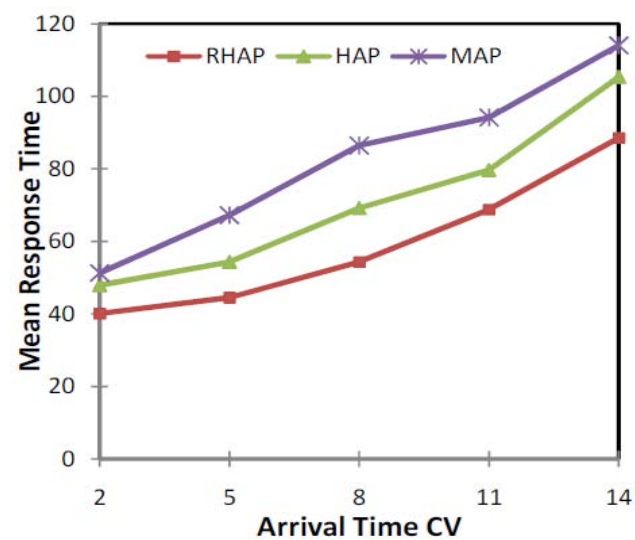


Fig. 2 : Sensitivity to arrival time CV

b) *Sensitivity Analysis*

In this section, we study the sensitivity of the three policies to variances in inter-arrival and service times. When the arrival CV is varied, the service CV is held at 4. Similarly arrival CV is fixed at 1 when the performance sensitivity to service time CV is studied. The system utilization for parallel load is fixed at 80%.

i. *Sensitivity to Arrival Time Variations*

The performance sensitivity of the three policies to inter-arrival CV is shown in figure 2. The mean response time increases with increasing inter-arrival CV for the three policies. The RHAP policy maintains its performance superiority over HAP and MAP policy at 80% system utilization.

The increase in arrival time variance means the clustered arrival of jobs into the system. This also led to longer gaps in the job arrivals. The impact of variance in arrival time is more on HAP and MAP policies as shown in figure 2. These two policies suffer from processor fragmentation induced by the background workload and the way the partition-size is computed for the jobs. Since the partition sizes are computed on the basis of total number of BPUs (in case of HAP) and total number of processors (in case of MAP), the actual number of available BPUs (in case of HAP) and available processors (in case of MAP) can be lower than the partition-size computed. This is due to the fact that there is possibility of background tasks running on some of processors at the time and both HAP and MAP doe not consider background workload when computing partition size. But RHAP policy tend to produce smaller partition sizes due to consideration of background workload as well as upper limit imposed by Max parameter, therefore the impact of arrival time variance is reduced as compared to other two policies.

ii. *Sensitivity to Service Demand Variations*

The figure 3 shows that MRT of the three policies increases with the increase in the variance in the service demand. With the increase in service demand variance, there will few large service demand jobs and large number of small service demand jobs. As the service time CV increases, the service demand of the larger jobs will increase even though their number goes down as a fraction of the total jobs.

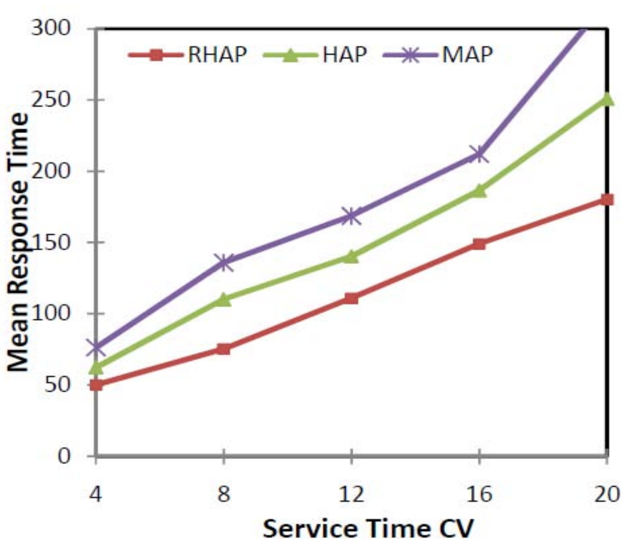


Fig. 3 : Sensitivity to service time CV

The impact of service time variance on three policies is more than the impact of arrival time variance. This is due to the fact that all of these policies use FCFS as a job selection policy which is known to be sensitive of variance in service demand, to allocate processors to jobs. FCFS allocation of processors to jobs results in a situation where small jobs could be blocked by an earlier arrived large job. This problem gets more serious as the variance in service demand increases.

VII. Conclusion

Space-sharing algorithms are preferred in distributed-memory cluster systems to avoid the overhead due to frequent preemptions involved in time-sharing systems. Adaptive space-sharing algorithms are used in distributed-memory parallel systems such as cluster computing systems and dynamic space-sharing algorithms are more suited to shared-memory multiprocessors. Most of popular adaptive algorithms are only designed for dedicated homogeneous parallel systems such as multiprocessors, PCC or even VCC type of clusters. Existing few adaptive algorithms for heterogeneous parallel systems require the knowledge of job characteristics to schedule jobs. This paper suggests a robust adaptive policy for non-dedicated heterogeneous cluster systems to schedule parallel jobs without requiring any knowledge of job characteristics. Comparative results have shown the dominance of the proposed policy over the existing similar policies at medium to high system loads of interest.

References Références Referencias

1. J.H. Abawajy. Parallel Job Scheduling Policies on Cluster Computing Systems. Ph.D. Thesis. Ottawa-Carleton Institute for Computer Science, Carleton University, Ottawa, Canada, November, 2003.
2. S.P. Dandamudi and Z. Zhou, "Performance of Adaptive Space-Sharing Policies in Dedicated Heterogeneous Cluster Systems", Future Generation Computer Systems, 20(5), 895-906 (2004).
3. D.G. Feitelson, L. Rudolph, U. Schwiegelshohn, K.C. Sevcik, P. Wong, Theory and practice in parallel job scheduling, in: Job Scheduling Strategies for Parallel Processing, Lecture Notes in Computer Science, vol. 1291, Springer-Verlag, Berlin, 1997, pp. 1–34.
4. D. G. Feitelson and L. Rudolph. Parallel Job Scheduling - A Status Report. Lecture Notes in Computer Science, Springer, Vol. 3277 (2005).
5. E. Rosti, E. Smirni, L. W. Dowdy, G. Serazzi, and B. M. Carlson. Robust Partitioning Policies for Multiprocessor Systems. Performance Evaluation, Vol.19, 141-265 (1994).
6. E. Rosti, E. Smirni, L.W. Dowdy, G. Serrazi, K.C. Sevcik, Processor saving scheduling policies for

multiprocessor systems, IEEE Transactions on Computers 47 (2) (1998).
7. S.P. Dandamudi and H. Yu, "Performance of Adaptive Space Sharing Processor Allocation Policies for Distributed-Memory Multicomputers", Journal of Parallel and Distributed Computing, vol. 58, pp. 109-125 (1999).
8. W. Cirne and F. Berman. Adaptive Selection of Partition Size for Supercomputer Requests. Lecture Notes in Computer Science, Springer, Vol. 1911, 187-208 (2000).
9. W. Cirne and F. Berman. Using Moldability to Improve the Performance of Supercomputer Jobs. Journal of Parallel and Distributed Computing, Vol. 62, 1571-1601 (2002).
10. W. Cirne and F. Berman. A Comprehensive Model of the Supercomputer Workload. Proc. of IEEE 4th Annual Workshop on Job Scheduling Strategies for Parallel Processing (2005).
11. S. Srinivasan, V. Subramani, R. Kettimuthu, P. Holenarsipur, and P. Sadayappan. Effective Selection of Partition Sizes for Moldable Scheduling of Parallel Jobs. Lecture Notes In Computer Science, Springer, Vol. 2552, 174- 183 (2002).
12. S. Srinivasan, S. Krishnamoorthy, and P. Sadayappan. A Robust Scheduling Strategy for Moldable Scheduling of Parallel Jobs. Proc. of 2003 IEEE International Conference On Cluster Computing (2003).
13. Young-Chul Shim, "Performance evaluation of scheduling schemes for NOW with heterogeneous computing power", Future Generation Computer Systems. 20(2): 229-236 (2004).
14. V.H. Doan. An Adaptive Space-Sharing Scheduling Algorithm for PC-Based Clusters, Modeling, Simulation and Optimization of Complex Processes, pp 225-234, 2008.
15. J.H. Abawajy, "An Efficient Adaptive Policy for High-Performance Computing", Future Generation Computer Systems, Vol. 25, 364-370, (2009).

Global Journal of Computer Science and Technology
Cloud & Distributed
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Test Automation with Distributed Database Systems

By Dr. R. Mahammad Shafi & Mungamuru Nirmala
Sree Vidyanikethan Engineering College, Tirupati, Chittoor (Dist), A.P, India

Abstract - Our previous research paper 'A Focus on Testing Issues in Distributed Database Systems' led us to a conclusion that Distributed Database Systems supports many good engineering practices but there is still place for refinements. A Distributed Database (DDB) is formed by a collection of multiple databases logically inter-related in a Computer Network. Apart from managing a plethora of complicated tasks, database management systems also need to be efficient in terms of concurrency, reliability, fault-tolerance and performance. As there has been a paradigm shift from centralized databases to Distributed databases, any testing process, when used in DDB correlates a series of stages for the construction of a DDB project right from the scratch and is employed in homogeneous systems. In this paper, an attempt is made to describe the establishment of Performance Testing with DDB systems. It focuses on the need for maintaining performance and some techniques to achieve performance in DDB systems. Three sample web based systems are tested by using TestMaker, one of the open source software, in order to highlight the helpful role of performance in the context of testing. The strengths and weaknesses of chosen performance testing tools viz., TestMaker, OpenSTA, and httperf are discussed.

Keywords : distributed database system, testmaker, openSTA, httperf , performance testing, TPS.

GJCST-B Classification: C.1.4

PERFORMANCE TEST AUTOMATION WITH DISTRIBUTED DATABASE SYSTEMS

Strictly as per the compliance and regulations of:

Performance Test Automation with Distributed Database Systems

Dr. R. Mahammad Shafi [α] & Mungamuru Nirmala [σ]

Abstract - Our previous research paper 'A Focus on Testing Issues in Distributed Database Systems' led us to a conclusion that Distributed Database Systems supports many good engineering practices but there is still place for refinements. A Distributed Database (DDB) is formed by a collection of multiple databases logically inter-related in a Computer Network. Apart from managing a plethora of complicated tasks, database management systems also need to be efficient in terms of concurrency, reliability, fault-tolerance and performance. As there has been a paradigm shift from centralized databases to Distributed databases, any testing process, when used in DDB correlates a series of stages for the construction of a DDB project right from the scratch and is employed in homogeneous systems. In this paper, an attempt is made to describe the establishment of Performance Testing with DDB systems. It focuses on the need for maintaining performance and some techniques to achieve performance in DDB systems. Three sample web based systems are tested by using TestMaker, one of the open source software, in order to highlight the helpful role of performance in the context of testing. The strengths and weaknesses of chosen performance testing tools viz., TestMaker, OpenSTA, and httperf are discussed.

Keywords : distributed database system, testmaker, openSTA, httperf , performance testing, TPS.

I. Introduction

A DDB is formed by a collection of multiple databases logically inter-related in a computer network [4]. In a distributed database, the network must allow users to share the data as transparently as possible, yet must allow each node to operate autonomously, especially when network linkages are broken or specific nodes fail. The transparences provided by a DDBMS can be understood as the high level semantic separation of the details inherent to the physical implementation of a DDB. The focus is to provide data independency in a distributed environment.

This way, the user sees only one logically integrated image of the DDB as if it were not distributed. Performance evaluation of database systems is an important concern. However, easier said than done, performance evaluation of database system is a non-rivial activity, made more complicated by the existence of different flavors of database systems fine tuned for serving specific requirements. However performance analysts try to identify certain key aspects generally desired of all database systems and try to define benchmarks for them.

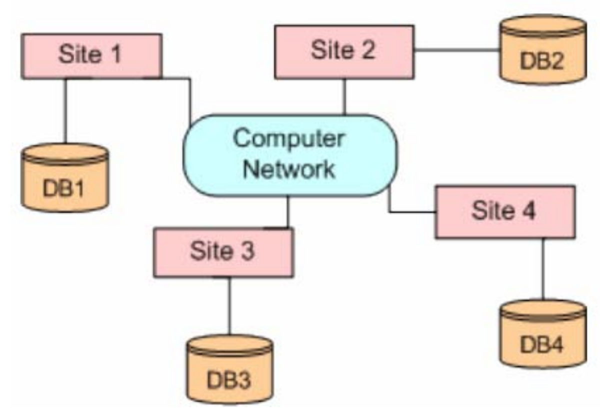


Fig. 1 : A Distributed Database on geographic dispersed Network

II. Overview of Performance Testing in DDB Systems

Distributed applications have traditionally been designed as systems whose data and processing capabilities reside on multiple platforms, each performing an assigned function within a known and controlled framework contained in the enterprise. Even if the testing tools were capable of debugging all types of software components, most do not provide a single monitoring view that can span multiple platforms. Therefore, developers must jump between several testing/monitoring sessions across the distributed platforms and interpret the cross–platform gap as best they can. Testing distributed applications is exponentially more difficult than testing standalone applications.

Neuman [2] categorizes three different dimensions used to measure the Performance of a system, viz., the size of the system, geographical performance, and administrative performance. These measurements ensure that although the users and resources may lie far apart, it is still easy to manage.

Performance testing provides the information regarding whether the system can still function in a fast

Author α : Professor & Head, Department of Master of Computer Applications, Sree Vidyanikethan Engineering College, Tirupati, Chittoor (Dist), A.P, India. E-mail : rmdshafi@gmail.com
Author σ : Research Scholar, Department of Computer Science and Engineering, Senate House,University of Allahabad, Allahabad, U.P.India. E-mail : nirmala.mungamuru@gmail.com

manner under heavy load. This information assists the IT manager to decide about the inclusion of additional servers. Tanenbaum and Steen [5] discussed a number of issues caused by performance. Centralized services, data, and algorithms can become problematic when the number of users increases. Although having a single server to serve a large number of users is not a good idea, adding additional servers to increase the system performance is also not practical in some situations. For example, the information on the server is highly confidential, such as information about bank accounts; adding additional servers create more chances for security attacks.

Another issue is geographical performance which also slows down the communication between clients and server. There are some techniques that can help to maintain and improve performance of distributed database systems. The most common technique is replication which adds more and faster processors as well as design components to be scalable [6]. Several copies of the same server are made available, the requests are sent to the servers based on their physical location, the loads of the server, or can be sent randomly. Consistency should be taken into consideration when this technique is used. It is to ensure that users can only view the up-todate information and the information appears the same to all users. This technique is not suitable when handling sensitive data, which was mentioned in the previous section.

Neuman proposed another technique which is known as distribution [5]. Distribution allows a component to be split into smaller parts which can be spread across the system. For instance, a name space is divided into different parts and a part of the naming database is assigned to different servers. Hence, it reduces the number of queries and updates to be processed; also each request is handled faster since the size of the database is smaller. Caching technique is also introduced by Neuman which allow the result to be remembered, thus, additional requests for the same information can be reduced.

According to Tanenbaum and Steen, hiding communication latencies technique can be used to enhance the performance of a system [5]. That is to say, after the client sends the request, the client continues to do other tasks rather than wait for the response from the server. When the response arrives, the application is interrupted to complete the previous task.

III. Testing the Performance of Sample Web Based Systems

Web databases serve the back-ends of Web-Servers. Web databases are the classic examples of high load, high performance database systems. The OLC Assets, DCRR and Employee Directory are web based systems. These three systems are chosen as samples for the performance test which is to test how each server reacts when there is an increase in number of users. These tests aim to highlight the role of Performance testing in analyzing system performance.

These tests also explain how performance testing can assist testers in making important decisions such as whether the current server(s) are able to serve an increase in the number of concurrent users, or whether additional servers should be implemented in order to handle a high volume of users.

a) OLC Assets

Otago Language Centre receives a number of new items every day to facilitate students in studying English [3]. These items can be library books, hardware, software, TVs, desks, chairs, etc., whose details are stored in the Center's database for future maintenance. OLC Assets System is a web based system that grants user's access to enter details of each item into the database by completing a simple form. The performance of the system is tested under the situation where there are multiple users who have entered a number of items into the database. Figure 2 illustrates the scalability index and XSTest performance index in the context of virtual users and TPS.

b) DCRR

A web based system that provides access to the users to search for a particular restaurant, comment about a restaurant via an electronic evaluation form, and to add a new restaurant into the database. Figure 3 shows two main interfaces of the DCRR system. A number of virtual users accessing the system to add a new restaurant are taken as the scenario for this performance testing.

c) Employee Directory

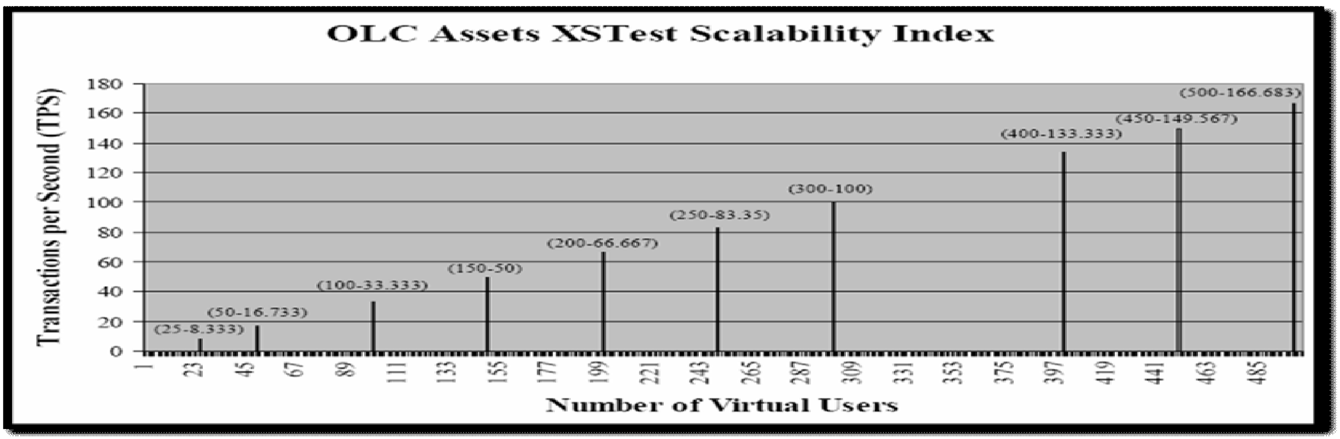
This web based system allows users to search for a particular employee and view the details of that employee. Two main interfaces of the system are shown in Figure 4. Performance testing is conducted in the situation where there are an increasing number of users searching for a particular employee.

IV. Test Results and Discussion

The three systems are tested using a range of concurrent virtual users (2 - 500) in one minute. Because of the limited resources, the maximum number of virtual users was set to 500. The output graphs (Figure 2, 3, and 4) which starts from 25 virtual users are redrawn based on the original graphs because as they do not show the ratio between number of virtual users appropriately. The original graphs are generated by TestMaker, one of the open source software that supports performance testing.

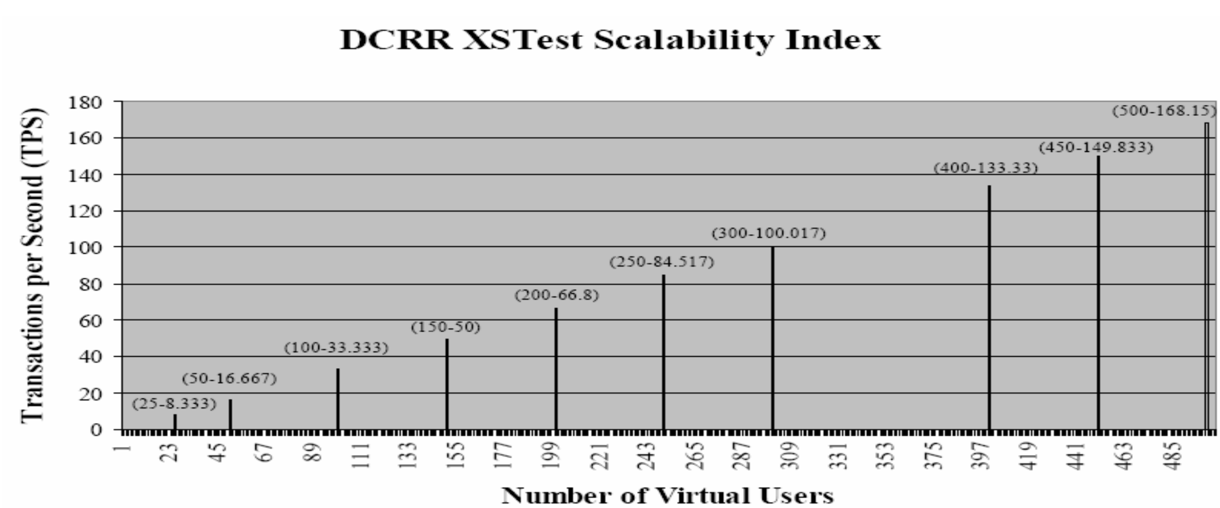
Each graph describes the number of successful transactions per second (TPS) versus the number of virtual users. The term "transactions per second" is defined as the number of pages per second a server can generate. It can be seen from the graph that as the number of users rises, the number of transactions per second gradually increases.

This indication shows that the server is still able to handle a large amount of concurrent requests. On the other hand, if the number of transactions per second drops as the number of users increases, which indicates that there is a concurrency problem and hence leading to performance problem. Although the results generated verify that the servers are still able to manage a large amount of concurrent requests; it is believed that when the number of users keeps growing, the server will fail to handle these requests at some point. Figure 2 illustrates the OLC Assets System – XSTest Performance Index, Figure 3 indicates the DCRR system performance index and Figure 4 shows the Employee Directory system performance
index.



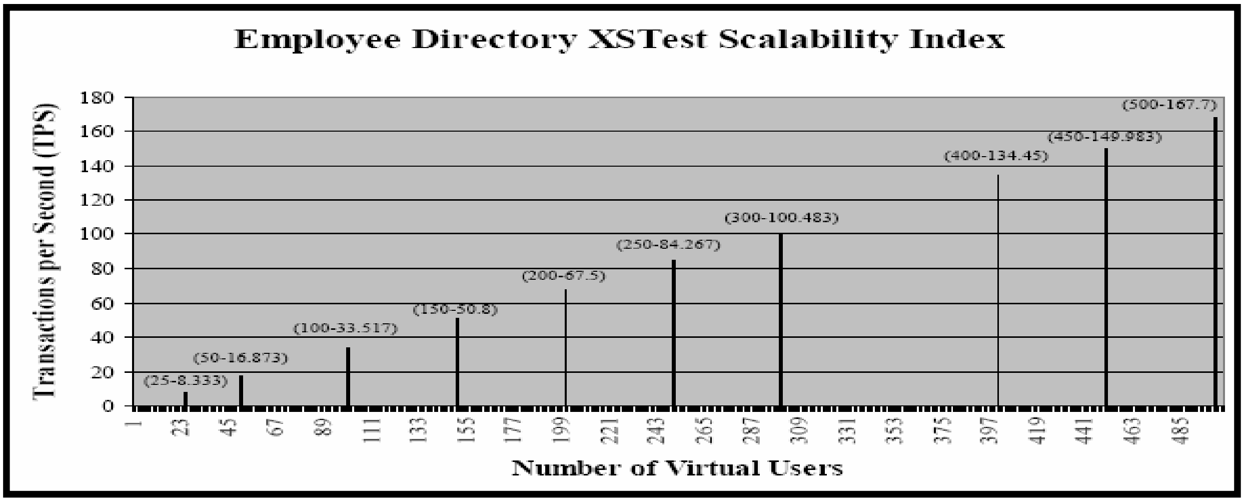
Number of Virtual Users	25	50	100	150	200	250	300	400	450	500
Transaction per Second (TPS)	8.333	16.733	33.333	50	66.667	83.35	100	133.333	149.567	166.683

Fig. 2 : OLC Assets System – XSTest Performance Index



Number of Virtual Users	25	50	100	150	200	250	300	400	450	500
Transaction per Second (TPS)	8.333	16.873	33.517	50.8	67.5	84.267	100.483	134.45	149.983	167.7

Fig. 3 : DCRR System – XSTest Performance Index



Number of Virtual Users	25	50	100	150	200	250	300	400	450	500
Transaction per Second (TPS)	8.333	16.667	33.333	50	66.8	84.517	100.017	133.33	149.833	168.15

Fig. 4 : Employee Directory System – XSTest Performance Index

V. Performance testing tools

The fact that performance testing helps in providing valuable information about the system's performance led to the development of number of performance testing tools. This section examines the strengths and weaknesses of three open source performance testing tools; viz., TestMaker, OpenSTA, and httperf.

a) TestMaker

It is a comprehensive testing framework that is used for performance, functionality, and load testing. A variety of test cases can be generated to perform thorough testing. TestMaker can support the Open Internet Protocols (HTTP, HTTPS, SOAP, XML-RPC, SMTP, POP3, IMAP, etc.). This software allows testers to create a number of virtual users and with the support from Test Network, testers can generate up to 10,000 or more concurrent test agents. TestMaker generates a clear output graph that represents the performance of the server based on the number of transactions per second versus the number of virtual users.

Apart from the strengths that are provided in the open source version, the commercial version offers some additional features such as the XSTest Pro that delivers performance index which helps to identify performance problems for capacity planning. Service Monitor System can send notifications via emails to notify, when a service fails or responds too slowly. Reports (charts and graphs) are generated to show the Performance index, result timing distribution, and performance timing by operation. This is an extremely useful feature since it is the quickest way to analyze the performance of the system. Another feature called Test Network, allows testers to generate a large amount of virtual users to test a specific web service.

On the contrary, TestMaker does have some weaknesses. Graphs are generated based on the number of transactions per second. In doing so, it assumes that all transactions are the same, even though some transactions may be long or short or complex. There is a possibility that a complex transaction may take shorter time to complete and this is not reflected on the graph. In addition, test cases should be performed more than one time to get the correct outputs.

b) OpenSTA

It is a completely free framework for testing the performance of Web Application Environments (WAEs). It is designed to create and run HTTP/S load tests in order to assess the performance of WAEs. OpenSTA provides a very simple GUI to create a new test, new collector, and a new script.

A new script is written in Script Control Language (SCL) and created by recording a list of activities that are carried out by the users. According to OpenSTA documentation [5], the process of creating collectors involves "deciding from which host computers or other devices performance data has to be collected and the type of data to collect".

After scripts and collectors are created, they are added into a test. Each test can be edited and controlled by using a number of features that are provided by the Graphical User Interface. These features include description about the test, start time, number of iterations, host name, number of virtual users, duration of the test, delay between each iteration, etc. Test can be monitored during execution and the result is displayed in graph when the test completes. Graphs can be customized to improve the presentation of data.

Finally, Easy to follow documentation along with online help and commercial support are provided by the vendors. One of the weaknesses is that OpenSTA can only support HTTP and HTTPS protocols; it can only run on Windows OS. Another difficulty is that testers have to understand the SCL language.

c) httperf

It is a tool for measuring web server performance. A test is executed at the command line by specifying hostname, port, page address, rate, number of connections, and timeout. Timeout features help testers to define the number of seconds that each client is willing to wait for the response from the server. When a test completes, the result is generated in the form of plain text. Mosberger and Jin explained that the output consists of six groups [1]. These groups covers the overall results, results pertaining to the TCP connections; requests that were sent; results for the replies that were received; CPU and network utilization figures and a summary of the errors that occurred. A performance graph is generated by httperf to illustrate the server performance. httperf has some weaknesses such as it only supports the HTTP protocol and can only run on a Linux OS. In addition, Mosberger and Jin point out that the testers have to start httperf on each client machine collect and summarize each clientresult. They also suppose that a single command line that can control multiple clients could help in improving httperf.

Table 1 : Comparative Analysis of performance Testing Tools

FEATURES	TOOLS		
	TestMaker	OpenSTA	httperf
Unix OS	✓		✓
MacOS X	✓		
Windows OS	✓	✓	
Support Junit Test	✓		
Commercial Version	✓		
Open Source Version	✓	✓	
Extensible Library of Protocols (HTTP, HTTPS, SOAP, XML-RPC, SMTP, POP3, IMAP)	✓	Only HTTP & HTTPS	Only HTTP
Friendly and easy to use GUI	✓	✓	
Support J2EE and .NET	✓		
Support for Test Result Analysis (i.e. graphs and charts)	✓	✓	
Object Oriented	✓		✓
Maintainability and Support	✓	✓	
Agent Recorder	✓	✓	
Sample Test Agent	✓		
Run Test from Command Line	✓		✓
Support for Virtual Users	✓	✓	✓
P2P Support			

Global Journal of Computer Science and Technology (B) Volume XII Issue XII Version I 13 Year 2012

GPL Open Source License	✓	✓	
Script Control Language		✓	
Transaction per Second	✓		
Calculate the rate of data transfer (bytes/sec)		✓	
Timeout Management		✓	✓

VI. Conclusion

A distributed database is not stored in its entirety at a single physical location. Instead, it is spread across a network of computers that are geographically dispersed and connected via communications links. A key objective for a distributed system is that it looks like a centralized system to the user. The user should not need to know where a piece of data is stored physically. Testing the performance of such an environment is really a typical task. Existing web-application performance-testing tools offer a broad variety of functionality. However, none of them combines all the functionality we expected to use in our projects. In an ideal world, everything works perfectly when the test is run. In reality, first runs often show problems in server configuration or in application itself. An effort has been made to test the performance of DDB systems like OLC Assets, DCRR and Employee Directory using some open source performance testing tools like TestMaker, OpenSTA and httperf.

References Références Referencias

1. Mosberger, D. & Jin, T., httperf – A Tool for Measuring Web Server Performance.
2. Neuman, B. C., Scale in Distributed Systems. Readings in Distributed Computing Systems. IEEE Computer Society Press.
3. OLC Assets System – University of Otago Language Centre. (2005).
4. R. Mahammad Shafi, Dr. B. Kavitha – A Framework for Designing and Testing a Distributed Database System, Proceedings of AMCM-2011.
5. Tanenbaum, A. S., & Steen, M. V., Distributed Systems – Principles and Paradigms. America: Prentice-Hall.
6. Emmerich, W. (1997). Distributed System Principles. UK: University College London.
7. Yuanling Zhu and Kevin Lu, Performance analysis of Web Database systems, LNCS, Volume1873/2000, pp 805-814, 2000
8. Codd, E.F., "A Relational Model of Data for Large Shared Data Banks". Communications of the ACM 13 (6): 377-387, 1970
9. Stonebraker, Michael with Moore, Dorothy. Object-Relational DBMSs: The Next Great Wave. Morgan Kaufmann Publishers, 1996.
10. Yao-S Bing, Alan R. Hevner, A Guide to Performance Evaluation of Database Systems, Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402,1984
11. Haran Boral, David J DeWitt, A methodology for database system performance evaluation, ACM SIGMOD Record, Volume 14, Issue 2, June 1984
12. Peter G. Harrison and Catalina M. Llado, Performance Evaluation of a Distributed Enterprise Data Mining System, Vol 1786/2000,pp 117-131, 2000
13. C. J. Date: "What is a Distributed Database System?" in Relational Database writings 1985-1989, reading, Mass:Addision-Wesley (1990).
14. Stefano Ceri and Giuseppe Pelagatti: Distributed Databases: Principles and Systems, New York, McGrawHill (1984).

Global Journal of Computer Science and Technology
Cloud & Distributed
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Key Distribution using Quantum Cryptography

By S.G.K Murthy, MV Ramana Murthy, M. Shuaib Qureshi, Mohamed Asslam Madathilakath & Mahaboob Sharief Shaik

Osmania University, Hyderabad, India

Abstract - Cryptography plays a vital role in Internet based applications. Present cryptographic systems on classical computers are providing sufficient security by utilizing symmetric and asymmetric cryptographic technologies but the advent invention of quantum computer makes the present asymmetric cryptographic systems vulnerable. The Quantum theory, which makes present cryptographic systems vulnerable, provides an alternative approach for secure key distribution. This paper depicts various issue related to conventional as well as quantum cryptography and secure key distribution using quantum cryptography.

Keywords : *cryptography, symmetric, asymmetric, security, key, quantum, photons.*

GJCST-B Classification: *D.4.6*

SECURE KEY DISTRIBUTION USING QUANTUM CRYPTOGRAPHY

Strictly as per the compliance and regulations of:

Secure Key Distribution using Quantum Cryptography

S.G.K Murthy [α], MV Ramana Murthy [σ], M. Shuaib Qureshi [ρ], Mohamed Asslam Madathilakath [Ѡ] & Mahaboob Sharief Shaik[¥]

Abstract - Cryptography plays a vital role in Internet based applications. Present cryptographic systems on classical computers are providing sufficient security by utilizing symmetric and asymmetric cryptographic technologies but the advent invention of quantum computer makes the present asymmetric cryptographic systems vulnerable. The Quantum theory, which makes present cryptographic systems vulnerable, provides an alternative approach for secure key distribution. This paper depicts various issue related to conventional as well as quantum cryptography and secure key distribution using quantum cryptography.

IndexTerms : cryptography, symmetric, asymmetric, security, key, quantum, photons.

I. Introduction

Information security is emerging filed in computing. Various security features are attained by using different cryptographic algorithms (symmetric and asymmetric). Present asymmetric cryptographic systems are based on certain hard problems, which cannot be solved in polynomial time. The key length is decided, such a way that it takes exponential time to break the key [1]. With the invention of quantum computers, proved that, it is possible to achieve enormous speed (computation) in solving certain hard problems. As a result current asymmetric cryptographic systems are not proficient of granting absolute security in near future. However the same quantum theory provides an alternative approach for absolute security [3]. This method of distributing, quantum key with the help of quantum physics can provide absolute security to information.

II. Present Cryptographic Systems

Presently there are two types of cryptographic systems available for confidentiality. In symmetric cryptographic systems, single key (secret key) is shared by the sender and recipient. These systems are not useful in large environment [2]. To overcome the with these systems, asymmetric cryptographic systems have been developed. In these systems pair of public and private keys is related mathematically with the property that the private key cannot be derived from public key.

Any information, which is encrypted by a public key, is decrypted only with the corresponding private key. This is a well-known method used by public key cryptographic systems to achieve confidentiality. As asymmetric cryptographic systems are based on very large number based computations and (unlike symmetric cryptographic systems) entire key is used directly in operation, the system becomes slower in encryption and decryption process. So these systems are used for secure key distribution as well as digital signatures.

Secure key distribution problem is solved by asymmetric cryptographic systems. Secret key can be used as a onetime pad. By using asymmetric cryptographic systems users can transmit secret key securely [5].

All asymmetric cryptographic algorithms are depending on a fact that certain mathematical functions can be done easily in one direction but not reverse. These types of functions are called trapdoor one-way functions.

RSA algorithm is a most famous asymmetric cryptographic algorithm that derives its strength from the hard problem, factorization of large composite numbers into two large prime integers. Factorization of very large integers is very difficult further it is exponentially growing, by adding each digit [4]. For a reasonable security, to be achieved, a 1024-bit key size is recommended in RSA cryptographic system. It is realized that for any asymmetric system, the ultimate strength lies on hard problem. Whether the hard problem is prime factorization or discrete logarithm, it takes enormous time for the present classical computers to break the key [6].

Presently, quantum and DNA based computing are newly emerging research areas, which facilitate faster computing. The invention of quantum computer has proved its strength in factorizing very large integers in polynomial time, which makes all asymmetric cryptographic systems vulnerable. To solve this problem, a new way of key distribution by using quantum physics has been proposed. This concept is based on certain fundamental properties of photons,

Author α : Scientist, D.R.D.O, Hyderabad, India.
Author σ : Chairman, Computer Science Department, Osmania University, Hyderabad, India.
Author ρ ¥ : Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Kingdom of Saudi Arabia. E-mail : qureshi.shuaib@gmail.com
Author Ѡ : Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Kingdom of Saudi Arabia.

like quantum entanglement, polarization of photons etc that provides absolute security.

An agreed random sequence of bits generated by quantum cryptography can be used as one time pad cipher, by using existing symmetric cryptographic system.

III. Quantum Physics

Photons (normal light) travel in the space with vibrations. The polarization of photon is the angle of vibration. The angle of vibration may vary in normal light even photons are travelling in the same direction. An un-polarized light is generated by normal light. We are considering four possible polarizations of photons in this paper, which are left, right, horizontal and vertical diagonals [1].

The orthogonal quantum states perception is raised by the two photons with vertical ('V') or horizontal ('H') polarization. 'V' and 'H' photons never pass from the polarizer that is destined for the other photon. Hence both 'H' and 'V' photons are two orthogonal quantum states of a photon [3]. Additionally 'H' and 'V' form a basis for the space of polarizations. Sending an un-polarized light through a Polaroid can generate a light of a particular polarization. The polarization of the polarized light is decided by the axis of the Polaroid.

In classical computers a bit has two logical states either 0 or 1. Unlike classical bits, quantum bits (qbits) can have two values at once. A qbit can exist in a coherent superposition of the two states. so that in quantum computers, one qbit can be encoded as 0 and 1 at any given moment. As L qbits are capable of storing 2^L numbers at time, a quantum computer performs massive parallel computation in a single operation on 2^L different numbers. To achieve the same task, it takes 2^L computations by classical computers. This feature helps quantum computers to factor large integers in polynomial time. Shor's algorithm facilitates efficient factorization of very large numbers by using quantum principles.

We cannot measure every aspect of a particle at the same time. The measuring of one aspect destroys the possibility of measuring the other aspect. This natural uncertainty is used as a concept to generate a secrete key. Further this secret key is used by utilizing symmetric cryptographic systems to achieve absolute security.

Considering the representation of binary numbers by orthogonal quantum states, quantum mechanics provide powerful new methods for information transmission.

IV. Quantum Concepts for Key Distribution

The author [7] states the photon polarization between Bob and Alice. If Alice polarized a photon in a given direction and Bob measured it in the same direction with Polaroid, the Bob acquires the photon with certainty. But random result will be acquired by Bob if he measures it is wrong direction depending upon the probability. So using quantum mechanics, how two parties could agree on a secret key is described as follows.

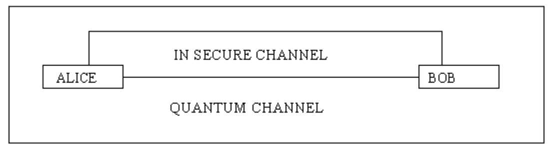


Fig. 1 : Key Distribution

Two communication channels i.e. insecure channel and quantum channel must be used by Bob and Alice for communication as shown in Fig.1.

For quantum bits communication, quantum channel is used, while as for symmetric cryptographic and general encryption, insecure channel is used.

Step 1 – Alice starts communication with the Bob by sending a series of randomly polarized photon.

Assume Alice communicates with the Bob by sending photons in the following polarizations.

| | \ — — \ — | / / | —

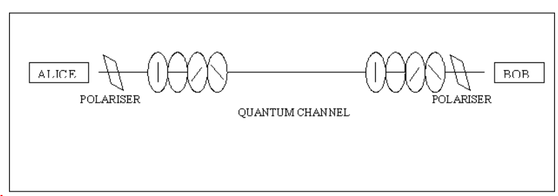


Fig. 2 : Quantum Channel Communication

Step 2 – At the Bob's side, there is a photons detector called as polarizer that detects the photons. For measuring the diagonal polarizations or rectilinear, Bob can amend the polarizer in any one direction. But due to the natural uncertainty of photons, this process is not doable for both.

Suppose Bob adjust his polarizer in the following directions corresponding to each photon.

Z + Z Z + + Z + Z + + Z

If the polarizer setting and the corresponding photon's polarization are matched with each other, then Bob gets the photon through the Polarizer. Suppose Bob acquires the below result,

Global Journal of Computer Science and Technology (B) Volume XII Issue XII Version I Year 2012

/ | \ / — | \ | / | | \

Step3 – Now Alice is informed by the Bob about the adopted setting using in-secured channel.

Step4 – Alice notifies Bob which settings are approved.

Step5 – Those polarizations are considered by Alice and Bob who were appropriately measured.

☆ | \ ☆ — ☆ ☆ | / ☆ | ☆

Then the photons polarization measurements are translated into bits using pre arranged code. The below string of bits is generated by translating the above commonly agreed polarizations,

0 0 1 0 1 0

0.5 is the average probability of estimating the correct polarizations. 2n photons are needed by Alice for generating n bits for transmission.

Step 6 – The integrity of the bit string is checked by Alice and Bob using testing.

Step 7- If the integrity test is verified, the same bit string is used as one time pad. Else the above procedure is repeated.

Using the above scheme, Bennet and Brassard proposed an operational model of quantum key distribution. Quantum cryptography provides absolute security by exchanging a series of qbits through fiber optic link.

V. Conclusion

In this paper the factorization issue created by quantum computers and the way that quantum cryptographic system providing a method to achieve absolute secrecy by utilizing quantum key distribution is discussed. Presently quantum cryptography has already been demonstrated by using optical-fiber networks. Over long distance, transmission of polarized photons without the use of fiber optics is proved by the latest experiments, but digital signature is one of the important features, widely used for internet related applications, achieved by asymmetric cryptographic systems. As the invention of quantum computers makes the present asymmetric cryptographic systems vulnerable, there is a need to form a method to create quantum digital signatures. In comparison to classical bit storages, storing quantum states is more difficult and generation and verification of quantum digital signatures requires extensive research in this direction.

References Références Referencias

1. Singh, S. Code, The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography, Doubleday, 1999.
2. Schneier B, Applied Cryptography, John Wiley New York, 2000.
3. Zeilinger, A, Fundamentals of Quantum Information, Physics world, March 1998.
4. William Stallings, Cryptography and Network Security Principles and practices, Pearson Education Ltd, Delhi, 2003.
5. Stinson, D, cryptography: theory and Practice, CRC Press, 2002.
6. Omar M.B, A. Irshad Khan, Mahaboob S. Shaik, MV Ramana Murthy, “Secure Communication using Symmetric & Asymmetric Cryptographic Techniques” I.J. Information Engineering and Electronic Business, pp. 36-42, 2012.
7. SGK Murthy, M.V.Ramana Murthy, P.Ram Kumar, New Trends in Cryptography by Quantum Concepts, Advances in Computer and Information Sciences and Engineering, pp. 428-432, 2008.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Cloud & Distributed
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Secure Storage Services in Cloud Computing

By Ms. B.Tejaswi, Dr. L.V.Reddy & Ms. M.Leelavathi
Sree Vidyanikethan Engg College, Tirupati-AP, India

Abstract - Cloud computing is an emerging technology and it is purely based on internet and its environment. It provides different services to users such as Software-as-a-Service (SaaS), PaaS, IaaS, Storage-as-a-service (SaaS). Using Storage-as-a-Service, users and organizations can store their data remotely which poses new security risks towards the correctness of data in cloud. In order to achieve secure cloud storage, there exists different techniques such as flexible distributed storage integrity auditing mechanism, distributed erasure-coded data, Merkle Hash Tree(MHT) construction etc. These techniques support secure and efficient dynamic data storage in the cloud. This paper also deals with architectures for security and privacy management in the cloud storage environment.

Keywords : cloud computing, data correctness, distributed data integrity, auditing, security.

GJCST-B Classification: C.2.1

A SURVEY ON SECURE STORAGE SERVICES IN CLOUD COMPUTING

Strictly as per the compliance and regulations of:

A Survey on Secure Storage Services in Cloud Computing

Ms. B.Tejaswi [α], Dr. L.V.Reddy [σ] & Ms. M.Leelavathi [ρ]

Abstract - Cloud computing is an emerging technology and it is purely based on internet and its environment. It provides different services to users such as Software-as-a-Service (SaaS), PaaS, IaaS, Storage-as-a-service (SaaS). Using Storage-as-a-Service, users and organizations can store their data remotely which poses new security risks towards the correctness of data in cloud. In order to achieve secure cloud storage, there exists different techniques such as flexible distributed storage integrity auditing mechanism, distributed erasure-coded data, Merkle Hash Tree(MHT) construction etc. These techniques support secure and efficient dynamic data storage in the cloud. This paper also deals with architectures for security and privacy management in the cloud storage environment.

Keywords : cloud computing, data correctness, distributed data integrity, auditing, security.

I. Introduction

From the perspective of data security in cloud, this has always been an important aspect of quality of service. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. In [1], as cloud-based services continues to grow, it has become clear that one of the key barriers to rapid adoption of enterprise cloud services is customer concern over data security (confidentiality, integrity, and availability). According to sun micro systems, the concept of transparent security makes the case that the intelligent disclosure of security design, practices, and procedures can help to improve customer confidence. According to K Ren, C.Wang and Q.Wang (Ref [2]), cloud storage allows data owners to outsource their data to cloud. However owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In [3], the authors specified a new scheme called Proof of Retrievability (POR), is a kind of cryptographic proof and is designed to handle large file. In [4], the authors introduced a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The PDP model for remote data checking supports large data sets in widely-distributed storage systems.In [5], the authors specified third party auditing which is important in creating online service-oriented-storage economy. It allows customers to evaluate risks. Also the authors introduced two types of auditing mechanisms; those are internal auditing and external auditing. In [6], the authors introduced privacy-preserving protocols. To make storage services accountable for data loss, authors presented protocols that allow a third- party auditor to periodically verify the data stored by a service and assist in returning the data intact to the customer. Most importantly, protocols for privacy-preserving never reveal the data contents to the auditor. In [7], the authors dealt with data dynamics. In order to achieve efficient data dynamics authors improved the Proof of Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. In [8], the authors (Q. Wang, K. Ren, W. Lou, and Y. Zhang) proposed a novel dependable and secure data storage scheme with dynamic integrity assurance. Based on the principle of secret sharing and erasure coding, they first proposed a hybrid share generation and distribution scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components. In [10], the authors introduced the concept of an aggregate signature, and presented security models for such digital signatures, and given several applications for aggregate signatures. They have constructed an e-client aggregate signature from a recent short signature scheme based on bilinear maps. In [10], the authors described a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. They described different possible architectures for privacy management in cloud computing; given an algebraic description of obfuscation, one of the features of the privacy manager; and described how the privacy manager might be used to protect private metadata of online photos. In [11], the authors explored a newly emerging problem of information leakage caused by indexing in the cloud.

Author α : M.Tech Student, Department of CSE, Sree Vidyanikethan Engg College, Tirupati-517102, AP, India. E-mail : tej.519@gmail.com
Author σ : Professor, Department of CSE, Sree Vidyanikethan Engg College, Tirupati-517102, AP, India. E-mail : lakkireddy.v@gmail.com
Author ρ : M.Tech Student, Department of CSE, Sree Vidyanikethan Engg College, Tirupati-517102,AP, India.
E-mail : leela9.mullangi@gmail.com

They designed a three-tier data protection architecture to accommodate various levels of privacy concerns by users. According to the architecture, they developed a novel portable data binding technique to ensure strong enforcement of users' privacy requirements at server side.

II. Methods

a) *Concept of Transparent security*

According to NIST (National Institute of Standards and Technology)Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

i. *Definition of Transparent security*

Transparent security can be defined as appropriate disclosure of the governance aspects of security design, policies, and practices. A security policy explains the high level approach to security and typically represents an organization's executive management position on security and risk. The policy might state that user data will be protected from unauthorized access both while being stored in the cloud and while in transit. The security design might then go into more detail by specifying that file-level encryption will be used along with an identity management implementation that restricts access to stored data. Security practices might also drill down further, describing the processes for proper management of encryption keys. The actual implementation would then choose a specific encryption algorithm such as Advanced Encryption Standard (AES).

ii. *Transparent Security Principles*

The following transparent security principles help to identify the types of information that should and/or should not be disclosed. The following conditions are examples of when disclosure is recommended:

- Principle-1—Disclosure of common security policies and practices. Common security features such as the use of firewalls and encryption of data in transmission or at rest should be disclosed because they are considered basic security features that most security people would expect to be in place anyway.
- Principle-2—Disclosure when mandated. When disclosure is imperative due to a legal or regulatory requirement, then this disclosure must be performed.
- Principle-3—Security architecture. Security architectural details that may either help or hinder security management should be disclosed. For example, the implementation of secure by default configuration should be disclosed. However, if these types of details also create a security risk as described in other items below, disclosure would not be appropriate.
- Principle-4—Governance. It means responsibilities of the customer versus those of the cloud providers, should be clearly articulated so that the customers are clear on what they must do themselves to protect their data.

b) *Proof of Retrievability (POR) Model*

POR protocol encrypts F and randomly embeds a set of randomly-valued check blocks called *sentinels*. The use of encryption here renders the sentinels indistinguishable from other file blocks. The verifier challenges the prover by specifying the positions of a collection of sentinels and asking the prover to return the associated sentinel values. If the prover has modified or deleted a *substantial* portion of F, then with high probability, it will also have suppressed a number of sentinels. It is therefore, unlikely to respond correctly to the verifier. To protect against corruption by the prover of a small portion of F error correcting codes are there. Let F' refer to the full, encoded file stored with the prover.

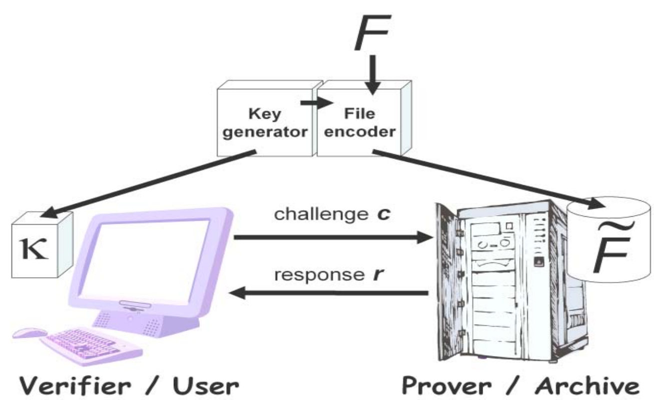


Fig. 2.2.1 : Schematic diagram of a POR system

An encoding algorithm transforms a raw file F into an encoded file *F* to be stored with the prover / archive. A key generation algorithm produces a key stored by the verifier and used in encoding.

c) *Provable Data Possession (PDP) Model*

Provable data possession (PDP) model provides probabilistic proof that a third party stores a file. The model is unique in that it allows the server to access small portions of the file in generating the proof; the above technique is used to access the entire file. Within this model, the authors (Ref [4]) give the first provably-secure scheme for remote data checking. The client stores a small O (1) amount of metadata to verify the server's proof. This model uses homomorphic verifiable tags. Because of the homomorphic property, tags computed for multiple file blocks can be combined into a single value. The client pre-computes tags for each block of a file and then stores the file and its tags with a server. At a later time, the client can verify that the server possesses the file by generating a random challenge against a randomly selected set of file blocks. Using the queried blocks and their corresponding tags, the server generates a proof of possession. The client is thus convinced of data possession, without actually having to retrieve file blocks. A PDP protocol checks that an outsourced storage site retains a file, which consists of a collection of n blocks. The client C (data owner) pre-processes the file, generating a piece of metadata that is stored locally, transmits the file to the server S, and may delete its local copy. The server stores the file and responds to challenges issued by the client.

d) Third Party Auditing (TPA)

Third Party Auditor: an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. The task of TPA is to verify integrity of the dynamic data stored in the cloud. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process.

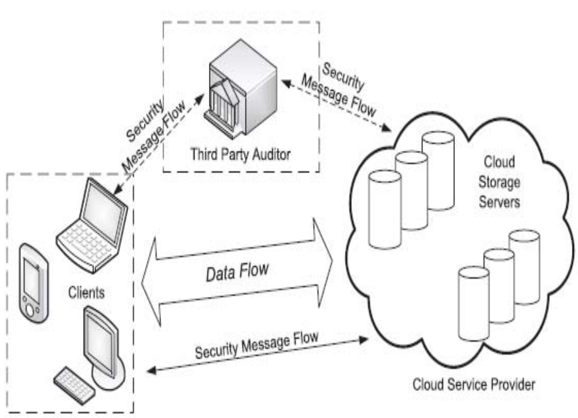


Fig. 2.4.1 : Cloud data storage architecture

e) Secret sharing and Erasure coding

Secret Sharing- Shamir proposed an *(m, n)* Secret Sharing (SS) scheme based on polynomial interpolation, in which *m* of *n* shares of a secret are required to reconstruct the secret.

Erasure Code -An *(k, n)* erasure code encodes a block of data into *n* fragments, each has 1/*k* the size of the original block and any *k* fragments can be used to reconstruct the original data block. Examples are Reed Solomon (RS) codes and Rabin's Information Dispersal Algorithm.

In the basic scheme, suppose a sensor node *v* has *data* to be stored locally. To protect *data*, it can perform the following operations to ensure the data integrity and confidentiality:

- **Step 1**: Generate a random session key *kr* and compute the keyed hash value *h*(*data, kr*) of *data*.
- **Step 2:** Encrypt *data*, *h* (*data, kr*) with *kr* and obtain *{data, h* (*data, kr*) *}kr* .
- **Step 3**: Encrypt *kr* using the key KUV shared between the authorized users and itself. This key can be either symmetric or asymmetric depending on the chosen user access control mechanism, which is independent to our design here and will not be discussed in this paper.
- **Step 4:** Store DATA $= <$ *{data, h*(*data, kr*) *}kr* , *{kr}KUV* $>$ and destroy *kr*.

III. Architectures

a) Privacy Manager in the Client

Privacy Manager Software on the client helps users to protect their privacy when accessing cloud services. A central feature of the Privacy Manager is that it can provide obfuscation and de-obfuscation service, to reduce the amount of sensitive information held within the cloud. Privacy Manager allows the user to express privacy preferences about the treatment of their personal information, including the degree and type of obfuscation used. Personae – in the form of icons that correspond to sets of privacy preferences – can be used to simplify this process and make it more intuitive to the user.

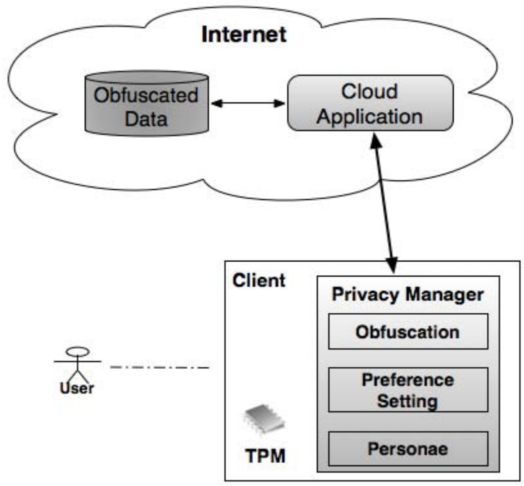
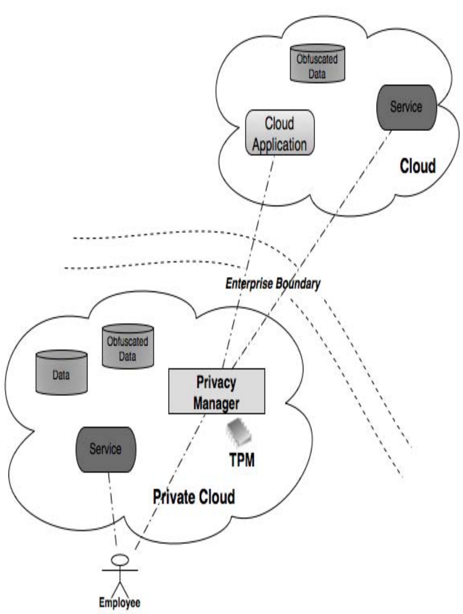


Fig. 3.1.1 : Client-Based Privacy Manager

b) Privacy Manager in a Hybrid Cloud

Privacy Manager may be deployed in a local network, or a private cloud, to protect information relating to multiple parties. This would be suitable in environments, such as enterprise environments, where local protection of information is controlled in an adequate manner and its principal use would be to control personal information passing to a public cloud.

Fig. 3.2.1 : Enterprise-focused Privacy Manager



Advantages to this approach include that the benefits of the cloud can be reaped within the private cloud, including the most efficient provision of the Privacy Manager functionality. It can provide enterprise control over dissemination of sensitive information, and local compliance. The Privacy Manager would act on behalf of the user and decide the degree of data transfer allowed, based upon transferred user policies and the service context, and preferably also an assessment of the trustworthiness of the service provision environment.

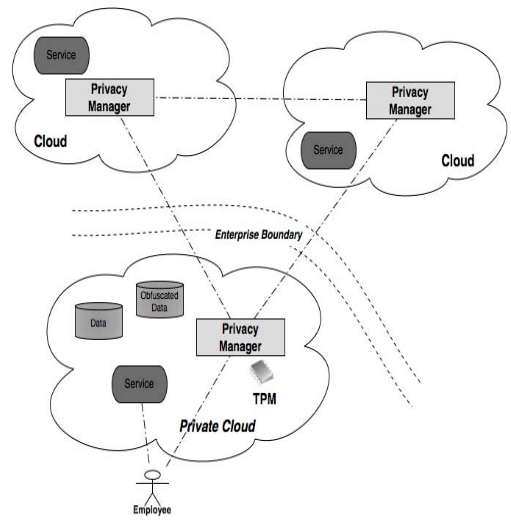


Fig. 3.2.2 : Privacy Manager within the Cloud

IV. Conclusion

This paper dealt with different security models to protect the data which is stored in the cloud. According to the user requirements, they may choose the most appropriate model. However, in the case of Third Party Auditing (TPA), cloud data storage security is critical because of its poor service quality. This paper also dealt with different architectural representations for privacy management. We provide the extension of the proposed one to support TPA, so that the users can safely delegate the integrity checking tasks.

References Références Referencias

1. Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https://www.sun.com/ offers/details/sun_ transparency.xml, White paper, Nov. 2009
2. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
3. A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, Oct. 2007.
5. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

6. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy- Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, http://eprint.iacr.org, 2008.
7. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.
8. Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. IEEE INFOCOM, pp. 954-962, Apr.2009.
9. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic techniques (Eurocrypt '03), pp. 416-432, 2003.
10. S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.
11. A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.

Global Journals Inc. (US) Guidelines Handbook 2012

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

PROCESS OF SUBMISSION OF RESEARCH PAPER

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION **<u>(Must be strictly followed)</u>**

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, “Abstract” word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript’s Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5.STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. **Pick a good study spot:** To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. **Think technically:** Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page

- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.

- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

CRITERION FOR GRADING A RESEARCH PAPER (COMPILATION) BY GLOBAL JOURNALS INC. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350