Ingress Defined Cloud Based Multivariate Retaliation Structure with Caching

[1]G.Janaki, [2]M.Menaka
Student
Kingston Engineering College, Vellore

***Abstract* - In the recent trends of computer world, cloud computing is a prominent computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Data sharing in form of multi-media is more complicated as it utilizes more traffic in the internet, hence the concept of multimedia streaming has been introduced. In the current technology, a cloud based storage system has been designed to distribute multi variant content (video, audio, doc, and image) with differential service level by utilizing a QOS algorithm. The enhancement is done by the cloud based storage system has been designed to provide multivariate services that serves the request by caching. Caching acts as an staging server in local machine that have temporary copy of the data that has been accessed frequently through LRU and MRU. Privilege setting has been incorporated with the system, that manages the accessibility of the data in cloud either publicly or privately. The cache is an area of cloud storage that is used to store content for dissemination.**

Keyword - Quality of Service (QoS), Least Recently Used (LRU), Most Recently Used(MRU),Threshold frequency value (TFV)

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Security issues in cloud concerns mainly associated with security issue faced by cloud service providers and the service issues faced by customers**.**

In cloud computing, users can outsource their computation and storage to servers (also called clouds) using internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g. Google Apps, Microsoft online), infrastructures (e.g., Amazon’s EC2, Eucalyptus, Nimbus) and platforms to help developers write applications (e.g., Amazon’s S3, Windows Azure).Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced.

When clients access multimedia objects from a content server, the content server must have sufficient disk and network to deliver the objects to the clients. Otherwise, it rejects the requests from the new clients. Thus, the popular content server can easily become the bottleneck in delivering multimedia objects. Therefore, server and network workloads are important concerns in designing multimedia storage systems over the Internet. Multimedia objects, like other traditional data files and Web pages, may betransferred across networks, such as the Internet. In order to provide efficientdelivery of data across the networks, some data can be stored in the middleof the network. When requests for the same object have been received, thesedata can be used to satisfy the requests at the middle of the network insteadof forwarding the request any further. This method to satisfy requests withpreviously accessed data is called caching. Since caching needs to consume a certain amount of storage space, the cache performance is affected by the size of the cache memory.

II. CREDENTIAL EXAMINING UNIT

User authentication process is required by the service provider whenever they use new cloud service.The service provider provides the user’s ID and access permission to the user after the user registration.When the user has been authenticated by the service provider, they can share the information on the cloud. Whenever the user shares the information, the service provider gives suggestion as the user is authenticated person to the server.

III. DATA ACCESS UNIT

The client will send multiple request to the server to check the availability of the service for sharing the information. The server accepts clients request and sends the response to the client if it is free or the requirement of the client is available. While responding to the client, the server checks the requesting client has authorization or not.To find the needed resources prepare metadata and dynamic statistical data which is needed for next step. Logical, detailed and protocol’s custom verification will be performed in this step. If the check fails or resources are not available, system will refuse to provide services and an error message will be generated to notify the user. The tricky part here is that since different resources are scattered in various places, system may not be able to obtain the resources needed in different environments and conditions. An important indicator here is how to properly handle different situations in order to provide robustness of the system to achieve the goal of fault tolerance.

IV. PRIMARY THRESHOLD SETUP

Client can share the any type of information on the cloud services with more security and lower cost. All the accessed data through cloud are stored in the local catch automatically. It is easy to retrieve the data from the local catch not from the main server. Hence accessing time will be reduced.

STEP 1: User enters the details in the registration forms.
STEP 2: The entered details is fetched as String data type and been identified as an identifier.
STEP 3: Through AES Encryption the user details is been encrypted into database.
STEP 4: The user pays to get privilege of High or Low Quality users.
STEP 5: Based on the payment amount the access codes are sent to the registered mail.
STEP 6: The user are made to use access code to enter the server for first time to verify the email.
STEP 7: Once verified the multivariate data such as (audio, video) are displayed by search preference.
STEP 8: If user have high quality privilege go to step 9 else go to step 10.
STEP 9: The video is displayed in form Most recently used as first then descending to the order.
STEP 10: The video is displayed in form least recently used as first then descending to the unviewed at last.
STEP 11: The high quality user have reduced buffer time of videos where as low quality user don’t have such privileges.
STEP 12: Log out and End the session.

V. BANDWITH SPECIFICATION

HIGH USERS	LOW USERS
1 sec=10 mb	1 sec=5mb
9sec=90mb	4.5=22.5mb

Figure 1.1 Classification of User Access Time.

Hqj= Hqj+Uq*((St-Sf)/Sf)
Hqj=10*((2sec-0.2)/0.2) //*high priority
=10*((1.8/0.2))
=10*(9)
Else
lqj= lqj+Uq*((St-Sf)/Sf)
Lqj=5*(2sec-0.2)/0.2) //* low user
=5*(*((1.8/0.2)) //*low priority
=5*(9)

Hence these units helps to provide the better efficiency in the result.It helps to serve the low class users in specified steps.

VI. DATA CACHE ALGORITHM

Multivariant data such as JPG,AUDIO,TEXTFILES can proposed by the Client-Server model.Cache frequently accessed user data’s are cached in the local server. The cache is an area of cloud storage that is used to store content for dissemination. The cache is mounted with in the system drive as a folder.The process of history cleanup has been done to the cache data’s in the staging invoked local server.A priority process of detection is carried out to erase off the cache details from the local server.Thus the proposed methodology is efficient as when compared to the existing and override the limitations.

Improved quality can be achieved by using vendors with more expertise and more specialized processes.Sharing an entire folder or a single file with other users can be easily carried out with few clicks of the mouse which makes it absolutely convenient and easy for the users.Storing files or data locally presents businesses with more security concerns whereas encrypted data on online storage services prevents unauthorized use or access in an easy way.Content delivery services, high server load, delay, un availability of videos and hardware complexity such as NAS,DAS,SAN can be reduced.

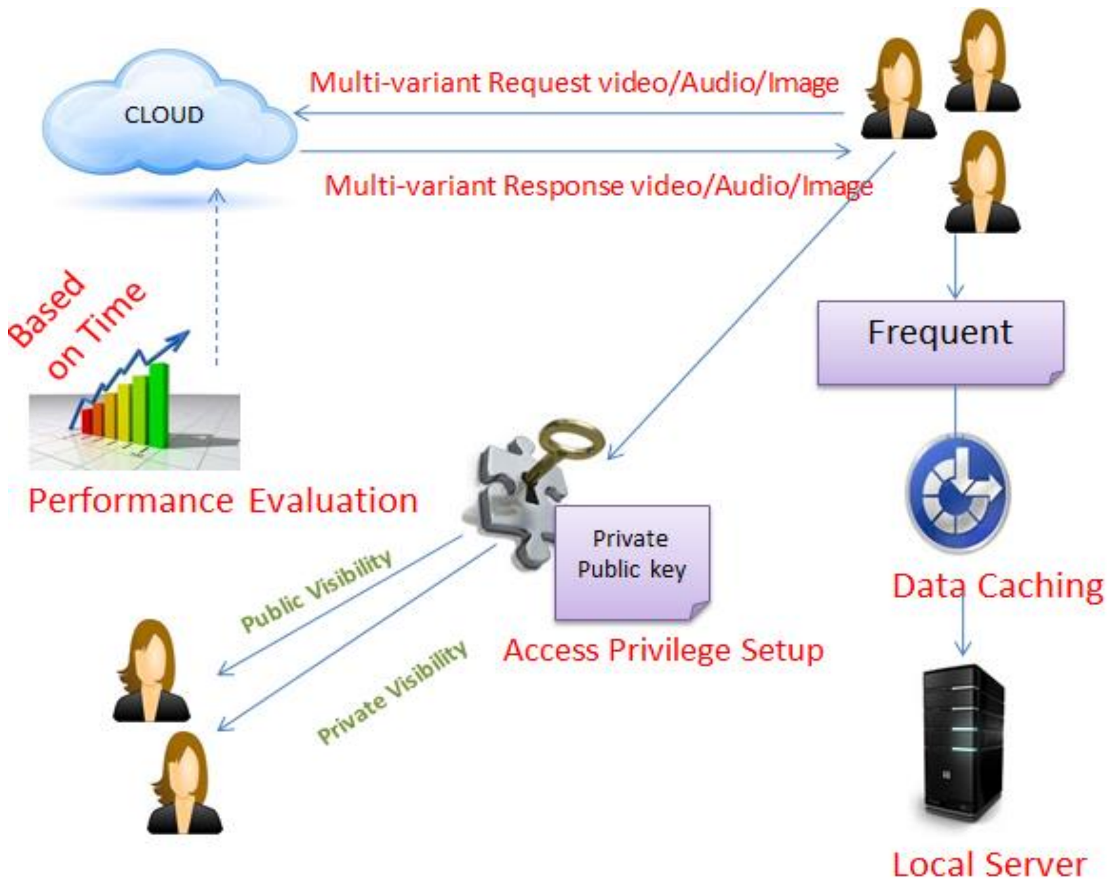

Fig 1.2 Proposed Architecture

Clients use to send the request to the cloud in order to access different video and audio. It can be easily done with a click of mouse using caching technique. Caching helps to store the multimedia files temporarily within a client side itself. It increases efficiency, bandwidth and threshold of the data when it is accessed by the user frequently. Frequent users are separated based on access privilege setup.

A cache algorithm is a detailed list of instructions that decides which items should be discarded in a computer's cache of information.Least Frequently Used (LFU): This cache algorithm uses a counter to keep track of how often an entry is accessed. With the LFU cache algorithm, the entry with the lowest count is removed first.

Least Recently Used (LRU): The oldest element is the Less Recently Used (LRU) element. The last used timestamp is updated when an element is put into the cache or an element is retrieved from the cache with a get call.

Most Recently Used (MRU): This cache algorithm removes the most recently used items first. A MRU algorithm is good in situations in which the older an item is, the more likely it is to be accessed.

Pseudocode

```
INPUT: threshold TSVH
INPUT:data transfer time Ti
If(cumulative>TSVH)
Remove FileID
Else
Provide FilePATH
```

APPROACHES FOR LRU

A.DYNAMIC THRESHOLD SETUP

Threshold value will be incremented by 1,each time when the video has been accessed.HU-TS value1 is reserved.Since TS is only allocated for high class users they have more usage on accessing the videos without any buffering.Other users such as LU don’t have any TSV.so each time the video has been streamed from the server. Low users cannot have any cache storage.

- First admin must upload multimedia content such as audio, video etc.,
- Once data’s are uploaded, It will be available for users by accessing the cloud
- Based on privilege access, threshold value will be set to maximum value of 10.

When TSV reaches to Maximum level (i.e., TSVH>10) FileID(path) will be removed.When TSV incremented to 9,the final threshold limit has been provide only to High class users-premium members.

Else.Final threshold value cannot be access to permit for low users.

B.LRU: It has been commonly known that after a data object or a stored program isaccessed, the probability that the same object or the same program is beingaccessed again within a short time is high. Therefore, the period of time thatan object has been accessed is being considered to increase the efficiency ofthe cache performance.The recency of an object is defined as the period of time from which an objecthas been accessed to the present time. When an object has been recently accessed,its recency is said to be high. When an object has not been accessedfor a long time, its recency is then low. The least recently used method removes the least recently accessed objectfrom the cache first. It stores a timestamp for each data object. The timestampshows the time when the object was last accessed. Thus, it uses the recencyhistory of the object as the cache value.

C.LFU: The least frequently used method uses the frequency of past object accessesto predict the future accesses. The objective of the method is to keep thehot objects in the local cache and remove the coldest objects when space isneeded.Thus, the LFU method uses the access frequency of the data objects as thecache value of the object. The cache value of an object can be defined asequal to the access frequency of the object.

Sample arrival rate of objects(multimedia files) has been depicted as follows:

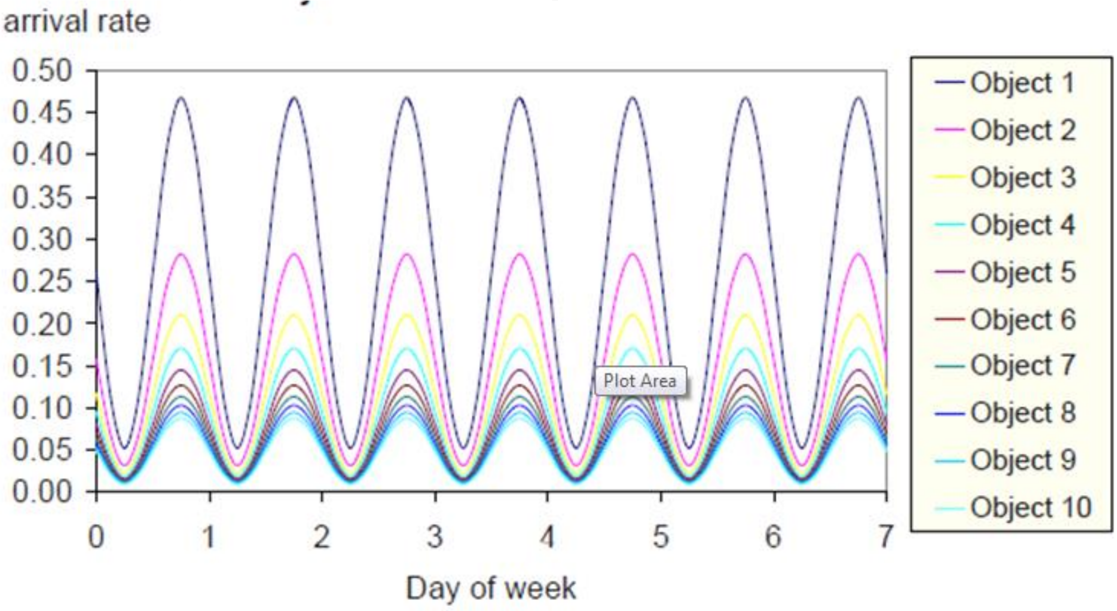

Figure 1.3Arrival rates of 10 objects

VII. AUTOMATIC CLEANUP SESSION

Local data catch will be invoked to store the frequently accessed data by the user.If the data are stored in the local catch, the user can access the data from local catch not from main server.It will reduce the accessing time and cost. Priority is the fact or condition of being regarded or treated as more important than others.According to the preference, the data will be deleted from the search history. In this module, we can share the any type of information on the cloud services with more security and lower cost.All the accessed data through cloud are stored in the local catch automatically.It is easy to retrieve the data from the local catch not from the main server. So that, can reduce the accessing time.

VIII. WORKLOAD MANAGEMENT

If the storage space is large, more objects can be stored on the cache storage and the probability of finding an object in the cache is thus high. The cache performs better. If the storage space is limited, only a few objects can be stored in the cachestorage, and the probability of finding an object in the cache is low. As a result, the cache performancebecomes low. Therefore, the cache size influences the cache performance. Since caching stores some previously fetched objects on the storage devices, the presence of an object exists on the storage devices significantly affects the efficiency of the caching. When a new object is being accessed, the cacheadmission policy decides whether an accessed object should be stored ontothe cache devices.Since the cache performance increases monotonically with the number ofobjects in the cache, the cache storage space is often full in order to keepthe most number of objects in the cache. When an accessed object needs tobe stored and the cache space is full, the cache replacement policy decideswhich object should be deleted from the cache storage to release space.

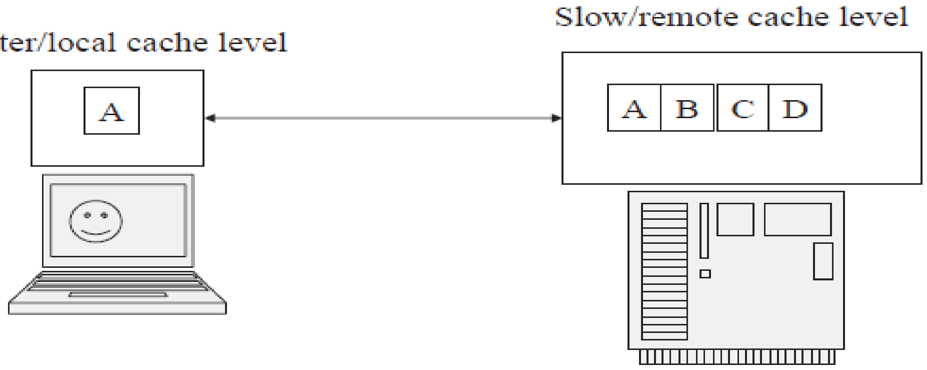

Figure 1.4 Memory caching is achieved by two copies of storage levels

IX. RESULTS AND DISCUSSION

A.EFFICIENT LOAD BALANCING

Rough calculations are provided based on threshold values of Low and High class users. The maximum number of requests of each memcached server in 1 s is approximately 1000. If the proposed system doesn’t use this technology, then these requests will be performed in the database. There are few databases which can really afford more than one thousand requests per second. Another possible solution is that storing the metadata into local memory

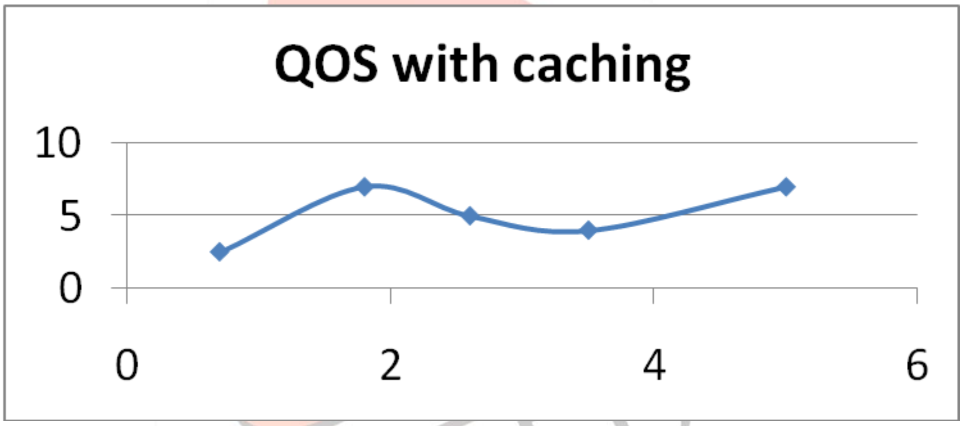

Figure 1.5 Manual load balancing graph

B.MAXIMUM CPU USAGE

It is quite typical and intuitive: system consumes more CPU resource when it serves more high class users. During the heavy load period (00:00–00:20), cds1spends more time on System which is the red area due to NFS service. Since NFS client runs in kernel mode, so cds1will spend more time on “System” when it needs more resources on the storage to serve increasing number of high class users. Needless to say, cds1 spends the most time on “IOWait” which is caused by accessing NFS storage and a little time on User which is caused by our content delivery service.

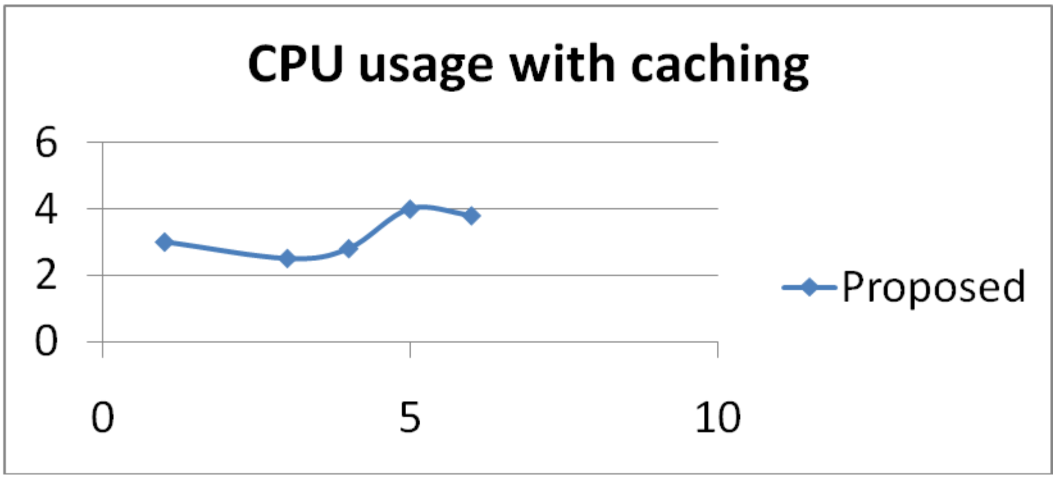

Figure 1.6 Manual usage graph

C. THROUGHPUT PERFORMANCE

The whole scenario of the experiment is that generating 50 Mbps download throughput of high class users in cds1 at the very beginning of the experiment. After 10 min, system starts to simulate very heavy throughput of low class users in cds2. From 21:50 to 22:30, low class users only use approximately 100 Mbps due to the limitation of constant Lt. From 22:30 to 23:00, system starts to generate another 50 Mbps throughput in cds1. During this period, high class and low class users use approximately 100 Mbps respectively, but throughput of low class users is slightly less than 100 Mbps due to the effect of constant Hr present this circumstance. From 23:00 to 23:50, system generates another 50 Mbps throughput again in cds1. Overall high class users use approximately 150 Mbps and low class users share the throughput which is lesser than 50 Mbps.

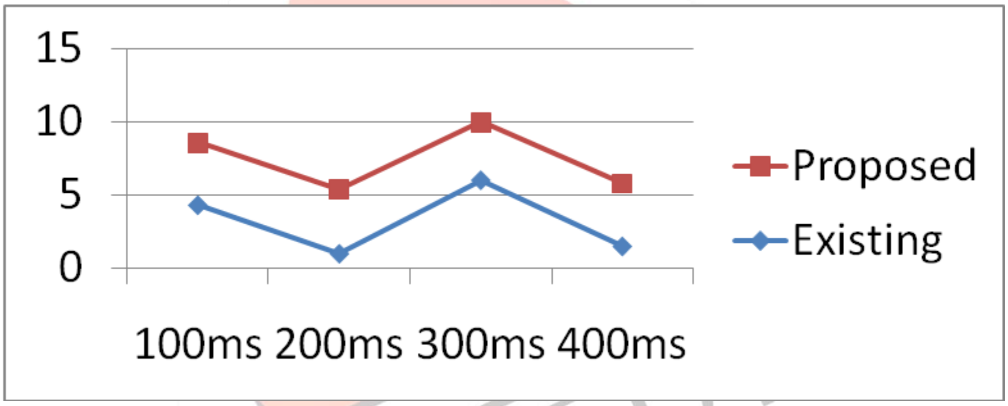

Figure 1.7 Manual storage throughput graph

D.CACHING PERFORMANCE

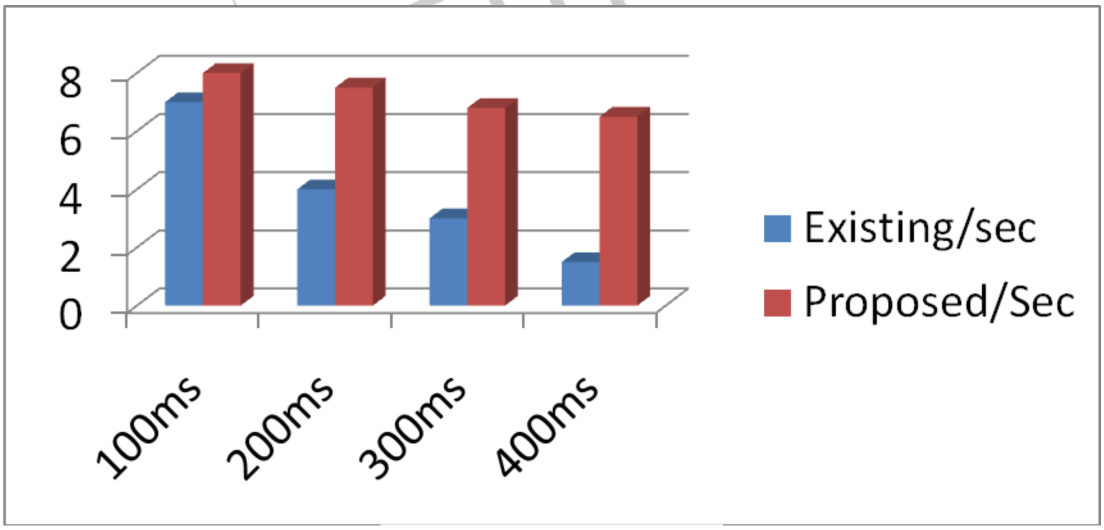

FIG 1.8 Caching performance

E.BANDWIDTH UTILIZATION

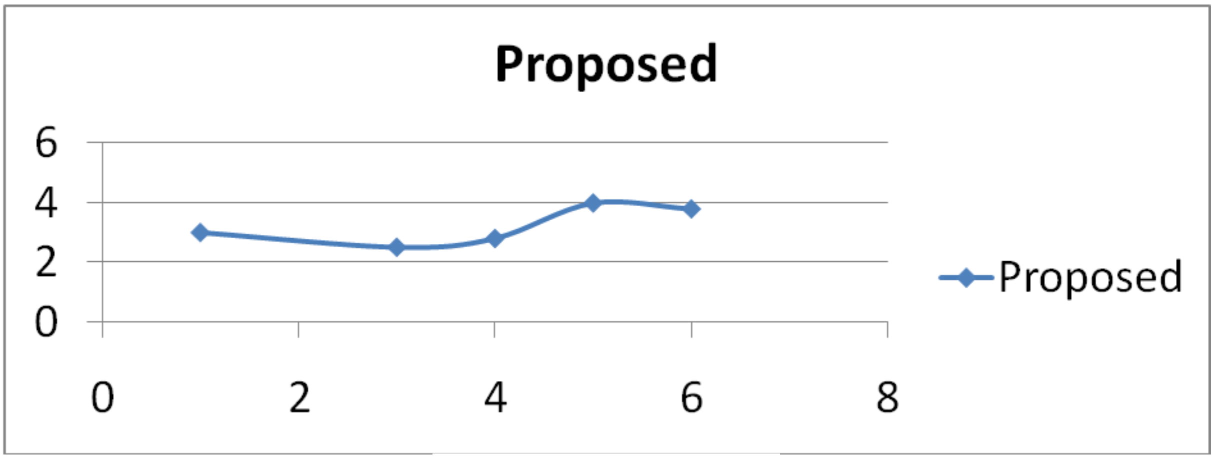

FIG 1.9 Bandwidth Utilization

G.EXPECTED OUTCOMES

Tasks	Existing	Proposed
Data storage(CLOUD)	Public to all users, admins	Public to only to owner of data
Communication	Disclosure can occur during Man in middle attack as only public key encryption(Hashing)	Hacker can be avoided as private ket(Using Gmail access code)
Login	User information are fetched only after submit button is clicked. The validation is carried out in server	User is validated by Id, password and admin also have right to block user if found duplicated information
Quality	All user have same level of priority it affects the premium users	Have better quality assurance for premium users

X. CONCLUSION

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed. Cloud resource management requires complex policies and decisions for multi objective optimization. It is extremely challenging because of the complexity of the system, which makes it impossible to have accurate global state information. Thus the proposed methodology is efficient as when compared to the existing technology.

XI. FUTURE WORK

There are some future works in the proposed system. Since system stores contents on storages randomly, the content scheduling algorithm could be developed in the future in order to balance the access load on all storages as far as possible and avoid hot-spot storage to a certain extent. Another issue is that whether some storage are ultimately popular and cannot even serve high class users properly. The content pieces caching algorithm may be developed in the future in order to solve this issue and improve overall system performance.

REFERENCES

[1]. 2011 J. Somorovsky,et al., “All your clouds belong to us—security analysis of cloud management interfaces,” ACM Comput. Commun.Security Conf.

[2]. 2011 F. Zhang, et al., “CloudVisor: retrofitting protection of virtual machines in multi tenant cloud with nested virtualization,” Symp. Operating Syst. Principles.

[3]. 2012, S. Butt, et al., “Self service cloud computing,” in ACM Comput. Commun Security Conf.

[4]. 2012 V. Varadarajan, et al., “Resource freeing attacks: improve your cloud performance (at your neighbor’s expense),” ACM Comput. Commun.Security Conf.

[5]. 2012 “Xen security advisory 19 (CVE 2012 4411)–guest administrator can access QEMU monitor console.” Available: http://lists.xen.org/archives/ html/xen announce/2012 09/msg00008.html

[6]. 2013 Amazon Inc., “Amazon elastic compute cloud (Amazon EC2),”. Available: http://aws.amazon.com/ec2/

[7]. 2013, K. Beaty, et al., “Network level access control management for the cloud,” in IEEE Int. Conf. Cloud Eng.

[8]. 2013, C. Yu, et al., “Protecting the security and privacy of the virtual machine through privilege separation,” Int. Conf. Comput. Sci. Electron. Eng.

[9]. 2013 “Windows Azure.” Available: http://www.windowsazure.com/en us/

[10]. 2014, Yen-Ming Chu et al,“Quality of Service Provision in Cloud-based
Storage System for Multimedia Delivery” Senior Member, IEEE SYSTEMS JOURNAL, VOL. 8, NO. 1, MARCH 2014