Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 22 Issue 1, January 2020

# Clustering Strategy Performance Analysis of Cloud DVR for Energy Efficiency

Mr. Rajesh Pandey, Vijay Maheshwari
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- rajesh@shobhituniversity.ac.in, vijay@shobhituniversity.ac.in

***ABSTRACT: Comcast's cloud digital video recorder (cDVR) is a new service available to its customers. In the Cablevision judgment, the main current legal interpretation allowing cloud DVR is based on a single copy. As a result, the cDVR data center's operating costs are very expensive. To save energy, an asynchronous service system with user classification based on cDVR use is used. CDVRs with comparable use schedules are built in one cluster in this system. If there have been no cDVR requests for a period of time, the cloud recording service on this cluster goes to sleep. When one or more cDVR requests arrive, they are delayed in queues until the cDVR service comes up. To evaluate the performance of this system, a 2-class Markov Geo vacation model is given in this article. In simulations and experiments, different scheduling strategies are compared. Distributed networking may help in situations where resource sharing is a problem or when greater fault tolerance is required. Higher degrees of anonymity are also well supported by distributed networking. Cloud computing is a kind of computing that uses thunder the conventional client/server computing paradigm, enterprises with fast growth and scalability requirements may find it difficult to manage their own distributed network***

***KEYWORDS: Cloud TV, Cloud Digital Video Recorder (cDVR), Energy, Efficiency, Markov Process.***

## 1. INTRODUCTION:

Cloud computing is getting more popular these days. Comcast offers a cloud TV service to its consumers, which provides them with two main benefits: viewing TV on any device, anytime, everywhere recording TV Movie programs in cloud digital video record (cdvr) so that people may access the cdvr to watch the videos later on any device. Because storing movies on a content delivery network is simple, the cdvr just needs to save the urns of recorded videos. However, each cdvr must give a tangible copy of any program that user’s record, as required by US legislation. As a result, the cdvr service is under a lot of stress. Aside from the hardware costs, everyday energy usage rises dramatically.

We use an asynchronous architecture of cdvr recording service to minimize energy usage. The use histogram has clustered the data. Users who have similar cdvr use patterns are grouped together in this system. This group's cdvrs are grouped together on a single server cluster. The cluster's cdvr recording service goes to sleep if there haven't been any requests for a time. Zhao has awoken. The recording requests are delayed in the two queues during the wake-up time. Those that record QAM videos go into the QAM queue, while those who record IP Streams go into the IP queue. For the cdvr recording service responding to QAM and IP streaming recording requests with a finite buffer, we used vacation modeling findings from queuing theory to estimate blocking probability and queue lengths caused by sleeping rules [1].

To the best of my knowledge, this is the first work on a 2-class vacation model, in which a server processes two classes of requests, each with its own buffer, while resting. The sleeping policy is generally divided into three categories How does the sleep cycle begin The exhaustive policy, in which the cDVR service does not go to sleep until the buffer is empty, is frequently employed. What happens at the conclusion of the sleeping process the most common methods are termination policy and threshold policy. In the previous strategy, the server only checks its buffer occupancy when it wakes up from sleep. It goes back to sleep if the buffer is empty. Otherwise, it will begin to handle requests. When the buffer occupancy changes, the latter policy needs the server to verify its buffer status. If the server's occupancy level rises over a certain level, it begins processing requests. What is the sleeping process' distribution typically; the sleeping process is modeled as a general distribution with a random variable that is independent and identically distributed [1].

The thorough, termination policy, and a procedure with the following are a breakdown of the paper's structure. A two-class vacation concept is presented in. The marginal occupancy distributions at each time instant are calculated. The numerical, computational, and experimental findings are presented in the conclusions. Model for a 2-Class Vacationed provide a model of a server that receives and processes 2-class heterogeneous requests in this section. Our method involves embedding a Markov chain in the time slot immediately after the processing of completion slots. The marginal occupancy distributions at processing completion slots are then calculated using equilibrium equations for the embedded Markov chain.

If the buffer is not full, requests from a certain class are queued in that buffer, otherwise they are blocked. Requests from the two buffers are chosen to be handled using a generic scheduling algorithm. The selection function, the likelihood that a class 1 request is selected to be processed, schedules the service order for requests of each class, while I and j requests are in class 1 and 2's queue, respectively. The processing procedure follows a standard pattern. When both buffers are empty at a process completion time instant, the recording service continues to handle requests [1].

## 2. DISCUSSION:

If there are no requests buffered waiting for processing at the sleeping termination time instant, the recording service goes to sleep and will continue to sleep’s previously stated, our analytical method entails embedding a Markov chain at the time instant immediately after the processing of completion slots, as is common for the system. We create two random variables [2].

When a sleep time ends, the server checks the two classes' buffer occupancies. If they're empty, a new sleep period will begin with independent Y. unless there are requests waiting in at least one of the two buffers at a sleep completion time instant, the procedure repeats. A sleep cycle is defined as the period of time between when a server or cluster goes to sleep and when it resumes processing requests. A sleep cycle, then, is made up of one or more sleep phases are the probabilities that I and Km requests of class m will come during a sleep cycle (Km). The fact that they are geometric distributions is obvious. it=1When both classes of requests come during the sleep cycle, the selection function selects a request from the two buffers at random using the general distribution [4].

So far, we've developed a computational method for calculating the equilibrium probabilities for a markov process embedded at processing completion time slots. we now proceed to the marginal occupancy distributions as observed at an arbitrary time slot, similarly to the study of a single class geo. We provide the findings directly to concentrate on the quantity of interest: buffer occupancies we only display portions of class 1's findings here due to space constraints. Class is identical to class 1. Due to a lack of space, the intricacies of the derivation are omitted here we can calculate the buffer occupancy for each of the two kinds of requests that arrive at the server under a sleeping policy using the equations above.

Following that, we provide numerical, computational, and experimental findings for this measure in three different scenarios: various wakeup speeds different buffer sizes different sharing percentages of a fixed-size shared buffer. We validate our modeling approach in this part by comparing numerical with simulation and experimental findings. Furthermore, we can determine the sleeping costs ofservers handling heterogeneous requests by changing the wakeup rate and buffer sizes of the two classes. First, we'll go through the setup of our simulations and experiments. The findings and comments on buffer occupancies will be presented later. The processing and sleeping processes have broad distributions in our model.

To demonstrate this, we use three different processing and sleeping distributions: exponential, uniform, and deterministic. Unless otherwise stated, the simulations and experiments are set up in the same way. We selected four scheduling strategies for the selection function I LJF stands for "longest job first. If class 2 is chosen. The amount of time it takes to process a task depends on whether there is an in-home check, parental control, TV rating check, and so on. Start with the shortest task. If I class 2 is chosen. HOL: class 2 has precedence over class 1; that is, class 2 requests are always processed first until its buffer is empty. The chance of selecting either class request is set at 0.5 in this case. Indicates that when the wakeup rate increases, the average occupancy of classes 1 and 2 falls and tends to remain constant after is higher than 1. The occupancy of LJF is higher than that of SJF in both classes [5].

The behavior is the consequence of surrendering some cost in the form of request processing delays. Because class 2 takes precedence over class 1, the average occupancy of class 2 is lower than that of class 1 owing to class 1's greater delay.it's clear that LJF has a higher average occupancy than SJF in both classes, regardless of buffer size. For HOL, similar results may be made. Due to the identical selection probability, BER performs similarly in both groups. While class 1's buffer size K1 is less than 5 , the occupancy of classes 1 and 2 rises as class 1's buffer size grows under LJF. Then the opposite happens: with rising K1, the occupancy of classes 1 and 2 decreases by 74 Z. Zhao. Changing the proportion of the common buffer that is shared only affects the saddle point, not the curve inclination [7].

### *2.1. Application:*

Because the service provider may access the data on the cloud at any moment, cloud computing raises privacy issues. It has the ability to change or erase data by mistake or on purpose. Many cloud providers may disclose information with other parties without a warrant if it is needed for law enforcement reasons. This is allowed under their privacy rules, which customers must accept before utilizing cloud services. Policy and regulation, as well as end-user decisions about how data is kept, are examples of privacy solutions. To prevent unwanted access to data processed or stored in the cloud, users may encrypt it. Identity management systems may also help cloud computing users deal with privacy issues [6].

These systems differentiate between authorized and unauthorized users and decide how much data each entity has access to. The systems function by generating and defining identities, tracking actions, and deleting identities that are no longer in use. Insecure Interfaces and APIs, Data Loss & Leakage, and Hardware Failure are the top three cloud security risks, according to the Cloud Security Alliance, accounting for 29 percent, 25 percent, and 10% of all cloud security outages, respectively. These come together to create a common set of technological flaws. It's possible that information belonging to various customers sits on the same data server on a cloud provider platform used by many users.

Furthermore, according to Eugene Schultz, chief technology officer of Emagined Security, hackers are devoting a significant amount of time and effort to finding methods to breach the cloud. "There are some genuine Achilles' heels in the cloud architecture that are allowing the bad guys to sneak in via the back door." Because data from hundreds or thousands of businesses may be housed on enormous cloud servers, hackers could potentially take control of massive data warehouses with a single assault, which he dubbed hyper jacking. with hackers stealing the credentials of over 7 million users in an attempt to extract monetary value in the form of Bit coins. They can access private material as well as have it indexed by search engines if they obtain these credentials [8].

The issue of ownership is often left out of many Terms of Service agreements. Physical control of computer equipment is more secure than having it off-site and under the management of someone else. This provides a significant incentive for public cloud computing service providers to emphasize the development and maintenance of secure services. Some small companies who don't have IT security knowledge may discover that using a public cloud is more secure. When signing up for a cloud service, there's a chance that end users won't grasp the problems. This is critical now that cloud computing is becoming more widely used and is needed for certain services to function, such as intelligent personal assistants.

Fundamentally, private cloud is regarded as more secure, giving the owner greater control; yet, public cloud is seen as more adaptable, requiring less time and money from the user. Bruce Schneider, a security expert, claims that "The disadvantage is that customization possibilities are restricted. Because of economies of scale, cloud computing is less expensive, and you usually get what you want when you outsource a job. A restaurant with a restricted menu is less expensive than hiring a personal chef to prepare anything you want. It's a benefit, not a problem, that there are fewer choices at a lower price." He also advises that "the cloud provider may not satisfy your legal requirements," and that companies should balance the advantages of cloud computing against the dangers.

Only the cloud provider has control over the back end infrastructure in cloud computing. Cloud providers often establish management rules that limit what cloud customers may do with their deployment. Users of the cloud are also restricted in their ability to govern and administer their apps, data, and services. This includes data limits, which are imposed on cloud users as a result of the cloud provider providing a certain amount of bandwidth to each client, and are often shared with other cloud customers. In certain activities, privacy and secrecy are major issues. For example, sworn translators operating under the terms of an NDA may encounter issues with sensitive material that is not encrypted.

In Cloud Computing, private information such as employee data and user data may be readily accessible to third-party organizations and individuals due to the usage of the internet. Many businesses benefit from cloud computing because it reduces expenses and enables them to concentrate on their core competencies rather than IT and infrastructure issues. Nonetheless, cloud computing has shown to have certain limits and drawbacks, particularly for small businesses, notably in terms of security and downtime. Technical outages are unavoidable, and they may happen when cloud service providers are overburdened while servicing their customers. This may lead to a temporary halt in operations. A person cannot access their apps, server, or data from the cloud during an outage since this technology's processes depend on the Internet. New developments Cloud computing is still a work in progress [9].

Chief technology officers wanting to reduce the risk of internal failures and the complexity of keeping network and computing gear in-house have been a driving force behind the development of cloud computing. They also want to exchange information in near-real time with employees in various locations, allowing teams to work together smoothly no matter where they are. Each year, major cloud technology firms spend billions of dollars on cloud research and development. Microsoft, for example, spent 90% of its $9.6 billion R&D budget on the cloud in 2011.

Centaur Partners, an investment bank, predicted in late 2015 that SaaS revenue will increase from $13.5 billion in 2011 to $32.8 billion in 2016. Due to the degree of data security and the flexibility of working choices for all employees, particularly distant workers, cloud technology has risen in prominence since the worldwide pandemic of 2020. Zoom, for example, increased by more than 160 percent in only 2020. According to Gartner, software as a service will continue to be the biggest market category for end-user cloud IT expenditure in 2021, growing 16 percent to $117.8 billion, while application infrastructure services will expand at a faster 26.6 percent to $55.5 billion Cloud-based digital forensics.

The difficulty of conducting investigations when cloud storage devices are not physically accessible has resulted in a number of modifications in how digital evidence is discovered and gathered. To formalize collecting, new process models have been created. Existing digital forensics tools may be used to access cloud storage as networked disks in certain cases. Another option is to use a program that runs entirely on the cloud. There is an option to utilize Microsoft's built-in e-discovery resources for businesses with a 'E5' subscription to Office 365, but they do not offer all of the capability that is usually needed for a forensic procedure [10].

## 3. CONCLUSION

ISSN: 0374-8588
Volume 22 Issue 1, January 2020

In this paper, we investigate the cost of implementing sleeping rules by applying the and vacation models to the cdrv server handling QAM and IP stream recording requests. The performance costs, notably queue length and latency, were calculated theoretically and are, in most instances, convergent. We discovered that the cost is unaffected by the processing time dispersion. We also discovered instances where the request arrival procedure and scheduling function had an impact on expenses. Decentralization is the antithesis of the client paradigm, in which any computer on the network may be utilized for the computing job at hand. Typically, only idle machines are utilized, and networks are believed to be more efficient as a result. Peer-to-peer computing is built on a distributed, decentralized network, which includes distributed ledger technologies like block chain. Mesh networking is a local network made up of devices that were initially intended to connect via radio waves, enabling for a variety of devices to interact. Every node on the network may communicate with every other node.

Computing was usually centered on a single low-cost desktop computer prior to the 1980s.However; today's computing resources are usually physically dispersed over a large number of locations, which is where distributed networking shines. Some forms of computation, such as Very Large-Scale Instruction Words, do not scale well beyond a certain degree of parallelism and the benefits of better hardware components, and are therefore bottlenecked. These constraints may be addressed by expanding the number of computers rather than the power of their components. Distributed networking may help in situations where resource sharing is a problem or when greater fault tolerance is required.

Higher degrees of anonymity are also well supported by distributed networking. Cloud computing is a kind of computing that uses theUnder the conventional client/server computing paradigm, enterprises with fast growth and scalability requirements may find it difficult to manage their own distributed network. The usefulness of distributed computing via Internet-based applications, storage, and computing services is known as cloud computing. A cloud is a collection of closely linked computers or servers that offer scalable, high-capacity computing or related services.

**REFERENCES**

[1] Z. Zhao, “Performance Analysis of Cloud DVR for Energy Efficiency Clustering Strategy,” 2014.

[2] A. Khoshkbar Sadigh, “Preparation of Power Distribution System for High Penetration of Renewable Energy Part I. Dynamic Voltage Restorer for Voltage Regulation Pat II. Distribution Circuit Modeling and Validation,” 2014.

[3] J. Son, R. Hussain, H. Kim, and H. Oh, “SC-DVR: A secure cloud computing based framework for DVR service,” *IEEE Trans. Consum. Electron.*, 2014.

[4] J. Ulm, “The dawn of cloud based DVR services,” 2014.

[5] D. Faltesek, “TV Everywhere? The Old Spatial Politics of New Media,” *Commun. Cult. Crit.*, 2011.

[6] H. Hietanen, “Networked digital video recorders and social networks,” in *2010 7th IEEE Consumer Communications and Networking Conference, CCNC 2010*, 2010.

*ISSN: 0374-8588*
*Volume 22 Issue 1, January 2020*

[7] M. Papish, “A method for implementing dynamic, cloud-based metadata services based on a unified content ID space across a fragmented CE ecosystem,” in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2012.

[8] Y. Zhang and B. Li, “A Novel Software Defined Networking Framework for Cloud Environments,” in *Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016*, 2016.

[9] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” *Comput. Electr. Eng.*, 2018.

[10] W. K. Hon and C. Millard, “Banking in the cloud: Part 1 – banks’ use of cloud services,” *Comput. Law Secur. Rev.*, 2018.