Cloud Bursting: Intelligent Technique in Cloud Computing

Dev Baloni[1], Sonu Pant[2], Mukesh Kumar[3], Gunjan Rawat[4], Shreya Rawat[5] and Puneet Kanti[6]
[1,2,4,5,6]Uttaranchal Institute of Technology,
Uttaranchal University, 248007, Dehradun, Uttarakhand, India
[3]Department of Computer Science & Engineering,
Graphic Era Hill University, Dehradun, Uttarakhand, India

2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART) | 978-1-6654-8734-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/SMART55829.2022.10047386

***Abstract*—Cloud Computing has been a difficult subject in the modern day for the past several years. The goal of cloud computing is to make resources and computation available through the internet. The process of deployment in cloud computing has several obstacles and challenges. This research article is primarily concerned with two topics: load balancing and cloud bursting. The best sort of algorithm covered here is the hybrid load balancing method, which was given by Shu-Ching. In this work, we also attempt to address the issue of high demand for diverse resources from industry and academics. To address this issue, we employ cloud bursting techniques, which allow us to give different servers to different customers and meet their demands.**

Keywords: Cloud Computing., Cloud Burst, Load Balancing Techniques

I. Introduction

The term ‘cloud’ comes from a computer network design that uses it to mask the infrastructure’s complexity. Delivering computing services through the Internet enables faster innovation, more adaptable resource management, and scale economies. Cloud stores and access data & applications via the internet. To put it another way, cloud computing is the greatest alternative for businesses for a variety of reasons, including increased performance, productivity, and cost savings. The name “cloud computing” refers to a method of accessing data that is remotely or digitally stored. Customers of cloud service providers have access to online storage of their programmes and files on remote servers. Since the user does not need to be in that particular location, they can access it from anywhere. Not all clouds are created equal, and not all cloud computing architectures are suitable in all circumstances. You can choose from a wide range of models, variations, and services to help you meet your needs. Before you begin building your cloud services, you must choose the cloud deployment or cloud computing architecture to be employed.

When computing demand spikes, cloud bursting allows a private cloud to access public cloud resources by “bursting” into a public cloud. As the need for processing power increases, an application that is now running in a private cloud or data centre will abruptly transition to a public cloud. This is referred to as cloud bursting.. An application that typically operates in a business’s on-premises data centre occasionally bursts onto a public cloud using a deployment technique called cloud bursting. This architecture may burst some or all an application’s processing units into the public cloud, depend on the exact situations. As a result, businesses may now use their own infrastructure for standard application workloads and transition to the cloud for heavy workloads. This makes it possible to control any unanticipated increase in processing demand [2]. A cloud infrastructure called a hybrid cloud includes two or more separate cloud infrastructures. Every year, “cloud bursting” becomes a more and more common practice [1]. You may save costs, improve operational efficiency, and boost performance and productivity with a cloud bursting architecture..

For non-critical, high-performance applications that work with non-sensitive data, cloud bursting is advised. An application can be started locally and burst to the public cloud to handle heavy demand, or it can be moved there to free up local resources for business-critical programmes. The applications that are best suited for cloud bursting are those that don’t need a complicated application delivery infrastructure or interface with other data centre applications, systems, or components. Cloud bursting can be advantageous for software development, large data modelling, marketing campaigns, analytics, and marketing campaigns. When considering cloud bursting, an organisation must think about security and regulatory compliance. One practical answer for stores that experience tremendous demand during the holiday shopping season, for instance, is cloud bursting.

The modern data user has little patience for interruptions in service, delays, or other excuses that prevent them from accessing the information they require when they need it. It is not difficult to imagine a time in the future when data and applications can freely navigate different resource configurations and dynamically self-assemble their ideal support infrastructure now that the major technological constraints have been identified. Although a fully seamless distributed architecture is still a work in progress.

II. An Outline of Cloud Bursting

In their 2009 definition of cloud computing, where they discuss the hybrid cloud architecture, the NIST briefly mentions cloud bursting as a method for load balancing between clouds. More details about cloud bursting and its uses are provided here. In the "cloud bursting" deployment model, an application typically runs in the on-premises data centre of an enterprise, but when specific conditions are satisfied, it bursts into a public cloud. This architecture may burst some or all of an application's processing units into the public cloud, depending on the exact circumstances. Companies can now employ their own infrastructure for routine application workloads while switching to the cloud for heavy workloads thanks to this. Thus, it is made feasible.

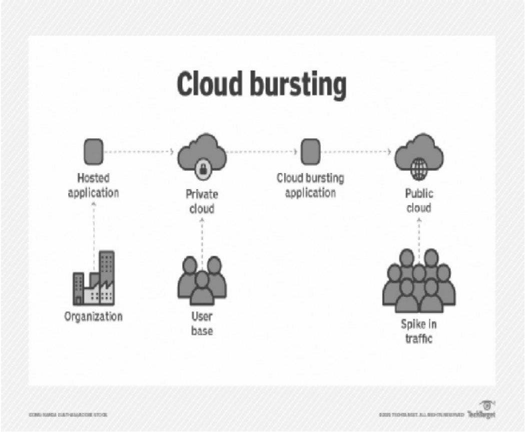

Fig. 1: Cloud Bursting Architecture

An organization's level of security, as well as any platform compatibilities and compliance needs, should be considered while adopting cloud bursting. Because private clouds are often more secure than public clouds, cloud bursting is not recommended for essential applications or data, as the data will be transferred across clouds. [5]

The table below summarises some of the primary business reasons why a company should use a cloud bursting architecture for specific applications.

Table 1: Commercial Drivers Intended for Cloud Bursting

Scenario	Description
Capacity Planning	An business calculates the manufacturing capacity required for its products to meet the constantly shifting market needs.
Organizational Agility	Organizational agility is the capacity of an organisation to quickly adapt to changes brought on by both internal and external sources.
Cost Reduction	To increase their overall corporate earnings, organisations reduce excessive spending.
Disaster Recovery /Fail Over	The on-premises installation of the application supports all users. In the event that some on-premises nodes fail, however, additional clients will be helped by public cloud instances.
Computing Requirement Spikes	Computing becomes more and more necessary. The computationally taxing parts of the application might be offloaded to the public cloud.

[6] examines the various aspects of effectively using cloud bursting for cloud professional models. Before introducing the cloud bursting paradigm, this essay emphasises the significance of effective workload classification as a component of enterprise design efforts. Workload transfer as part of cloud bursting is not effective for all workloads. The few methods for evaluating the cost-effectiveness of cloud bursting that have been proposed in the past [7] have primarily focused on the cost of cloud structure across cloud platforms rather than the total business benefits. In conclusion, the cloud burst deployment strategy must produce quantifiable business value. Consequently, the application evaluation process starts with a rigorous evaluation.

III. Load Balancing Solutions for Cloud Computing

Since load must be distributed fairly and dynamically among nodes in both private and public clouds, load balancing is ace of the biggest issues in hybrid cloud computing. By dividing workload among different nodes, load balancing in distributed systems aims to improve overall resource utilisation and task response time. Nodes are shielded from overload, kept active, and assigned tasks that are too simple for them [8]. The load on each node will always be roughly the same, according to the guarantee [9].

Shu-Ching et al. [11] presented a mixed load balancing policy. There are two phases to this policy. Static load balancing in stage one 2) Dynamic load balancing stage.

Algorithms for static load balancing According to Gulati et al. [10], load balancing for homogeneous resources is a prominent concern in the context of the cloud. The study of load balancing in a diverse setting is emphasised. By adjusting host bandwidth, VM bandwidth cloudlet long duration and VM image size, they used a dynamic way to assess the effects of the round-robin strategy. The variables associated with these parameters are used to optimise load. This implementation makes use of CloudSim.

For static load balancing, it selects a suitable node set, and for dynamic load balancing, it maintains a balance of tasks and resources. When a request is received, a dispatcher dispatches an agent to acquire information from the nodes, such as remaining CP

U capacity and memory. As a result, the dispatcher's job is to not solitary monitor and choose effective nodes, but also to allocate jobs to them.

Max–min, Min-min, and Suffer-age algorithms are some of the pre-selected heuristics for batch modes. As soon as a user request enters the scheduler in online mode, a computing node is selected to process the request. Because each task is only planned once, the scheduling result is unaffected. OLB, MET, MCT, and SA are some of the heuristics proposed for online modes. [13]

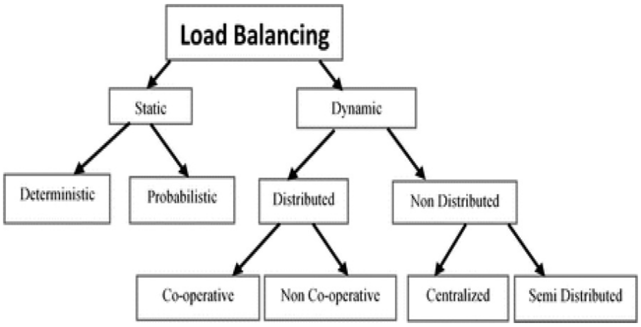

Fig. 2: Load Balancing Classification

In a cloud context, load balancing is done differently using ACO [12]. This study essentially proposed an ACO modification. Ants travel forward and backward to keep track of overloaded and underloaded nodes. Ants accomplish this by altering the pheromone, which carries information about the node's resources. 1) The foraging pheromone looks for a path to an overloaded node when it finds an underloaded node. 2) The trailing pheromone is used to locate a route to an underloaded node when an overloaded node is reached. The distinct result sets that the ants maintained in the previous method were eventually combined; in the current system, these result sets are often updated. Performance of the algorithm is enhanced.

A. *F5 Cloud Bursting Architecture*

The F5 Cloud Bursting solution manages the dynamic redirection of workloads to the best available location while automating and coordinating the deployment of application delivery services across traditional and cloud infrastructures.These application delivery services provide dependable user interfaces, adaptable workloads, and repeatable security controls.

Businesses can quickly, consistently, and dependably construct and manage application delivery services regardless of the underlying infrastructure thanks to F5 BIG-IQ Cloud, which federates administration of F5 BIG-IP solutions across traditional and cloud infrastructures. To speed up the overall application deployment process, BIG-IQ Cloud also interfaces with or communicates with current cloud orchestration tools like VMware vCloud Director.

BIG-IP GTM employs a range of sophisticated monitoring techniques with relation to each application and user in addition to global load balancing. It analyses the availability of the live application.

IV. Security Issues

Cloud providers are responsible for hiring and maintaining effective security methods in the cloud. To assuage their customers' fears about the cloud, these companies strive to persuade them that their data and apps will be properly protected [14]. Security is regarded as a serious stumbling block on cloud computing's path to success [15], and hence it is a big problem. Confidentiality, integrity, accessibility, authenticity, and responsibility are the five most essential core objectives for computer security. In the cloud computing paradigm, security is a major concern that has an impact on how extensively used the technology is [16]. The four-hour S3 (Simple Storage) network host service outage that occurred in 2010 made people more aware of the dangers that cloud-based data may face [17]. High-profile businesses like Amazon ,Google, Twitter and Microsoft continue to encounter network and application security threats such as hosts that have been infiltrated by botnets, data phishing, outages, data loss, weak passwords, and other incidents relating to conventional web and data storage security issues [18-19]

V. Conclusion

The paper is based on cloud computing concerns and challenges. Cloud computing is a skill that allows us to deliver a variety of services to customers, such as PAAS, SAAS, and IAAS, while also reducing a user's working time and providing a platform-independent environment. The key challenge in cloud computing is the security supplied to many users, as well as the high demands from industry, academia, and other organisations. To meet these high needs, we deploy cloud bursting technology, in which we assign separate servers to different users to meet their high demands. We presented a complete cloud bursting architecture in this work, which satisfies the demands of both public and private cloud customers. The need for cloud bursting is growing by the day in the modern period and meeting this demand will be a difficulty in the future. We also covered several load balancing parameters in order to properly divide their loads and flow network traffic.

References

[1] Birje, Mahantesh & Challagidad, Praveen & Goudar, R.H. & Tapale, Manisha. (2017). Cloud computing review: Concepts, technology, challenges and security. International Journal of Cloud Computing. 6. 32. 10.1504/IJCC.2017.083905.

[2] A. Zhygmanovskyi and N. Yoshida, &quot;Distributed Cloud Bursting Model Based on Peer-to-Peer Overlay,&quot; 2015 3rd International Conference on Future Internet of Things and Cloud, 2015, pp.823-828, doi: 10.1109/FiCloud.2015.74.

[3] K. K. Gopinathan, R. P. Pushpakath and S. K. Madakkara, "Quantitative assessment of applications for cloud bursting," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 1131-1136, doi: 10.1109/ICACCI.2015.7275762

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," Natl. Inst. Stand. Technol., Gaithersburg, MD, Spec. Pub. 800-145, 2009.

[5] D. Birkett and P. Miller, "Fit to burst: A practitioners guide to cloudbursting," Rackspace Whitepaper, June 2012.

[6] S. Reid, "Cloud bursting stimulates new cloud business models," Aug. 2011. [Online]. Available: http://blogs.forrester.com/stefan_ried/11-08- 08-cloud_bursting_stimulates_new_cloud_business_models

[7] T. Guo, U. Sharma, P. Shenoy, T. Wood, and S. Sahu, "Cost-aware cloud bursting for enterprise applications," ACM Trans. Internet Technol., vol. 13, no. 3, May 2014.

[8] Rimal, Prasad B, Choi E, Lumb V (2009) A taxonomy and surveyof cloud computing systems. Proceedings of 5th International Joint Conference on INC, IMS and IDC, IEEE .

[9] Sinha PK (1997) Distributed operating Systems Concepts andDesign. IEEE Computer Society Press.

[10] Gulati A, Chopra RK (2013) Dynamic Round Robin for Load Balancing in a Cloud Computing, International Journal of Computer Science and Mobile Computing 2: 274-278.

[11] Wang SC, Chen CW, Yan KQ, Wang SS (2013) The Anatomy Study of Load Balancing in Cloud Computing Environment. The Eighth International Conference on Internet and Web Applications and Services 230-235.

[12] Nishant K, Sharma P, Krishna V, Gupta C, Singh KP, et al. (2012) Load Balancing of Nodes in Cloud Using Ant Colony Optimization. Computer Modelling and Simulation 3-8

[13] Journal of King Saud University - Computer and Information Sciences
CrossRef DOI link to publisher maintained version: https://doi.org/10.1016/J.JKSUCI.2018.01.003

[14] Bernsmed, K. et al. (2012) ‘Thunder in the clouds: security challenges and solutions for federated clouds’, 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings.

[15] Bhaskar, P., Rimal, E.C. and Ian, L. (2009) ‘A taxonomy and survey of cloud computing systems’, Fifth International Joint Conference on INC, IMS and IDC, 978-0-7695-3769-6/.

[16] Ennajjar, I., Tabbi, Y. and Benkadour, A. (2014) ‘Security in cloud computing approaches and solutions’, 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), Tetouan.

[17] Zhang, S., Chen, X., Zhang, S. and Huo, X. (2010) ‘Cloud computing research and development trend’, Second International Conference on Future Networks, (ICFN 2010).

[18] Chen, Y., Paxson, V. and Katz, R.H. (2010) What’s New About Cloud Computing Security [online] http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html (accessed 14 March 2015).

[19] Subashini, S. and Kavita, J. (2011) ‘A survey on security issues in service delivery models of cloud computing’, Journal of Network and Computer Applications, Vol. 34, No. 1, pp.268–274.