WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Dynamic Load Balancing based on click stream

***Sneha.G*[#1], *Sangeetha Varadhan**[2]**

[#1] PGDepartment of Computer Applications,DR. M.G.R. Educational & Research Institute,Chennai-95,india
[1]snehagopal0304@gmail.com
[2]Assistant Professor
[#2] Assitant professorDepartment of Computer Applications,DR. M.G.R. Educational & Research Institute,Chennai-95,india
[2]sangeetha.mca@drmgrdu.ac.in

ABSTRACT :

Fog computing, a derivative of cloud computing, provides enhanced capabilities such as location awareness and deployment of datacenters at the network edge to effectively handle data in scattered networks. Dynamic load balancing solutions are essential for optimizing system efficiency and preserving system integrity. Nevertheless, previous research has failed to tackle authentication concerns specifically in edge datacenters prior to deploying load balancing solutions. This emphasizes the significance of security in distributed computing platforms. Static and dynamic load balancing techniques provide a conceptual foundation for comprehending various strategies used in distributed systems. The use of load balancing strategies such as First In, First Out (FIFO) and Last In, First Out (LIFO) is investigated in order to optimize the allocation of resources, reduce energy usage, and improve the overall performance of the system. The simulation findings demonstrate substantial improvements in resource allocation, affirming the efficacy of sophisticated load balancing systems in multi-data center settings.

Keywords— Load Balancing, Load Balance, Server, Server Over Load, Data Centers.

## Introduction

Load balancing is an essential technique in network computing that effectively distributes traffic over different servers or resources. This improves performance, ensures high availability, and prevents resource depletion. The technology has transitioned from conventional hardware-based solutions to contemporary software-based applications, often hosted in the cloud. These programs provide scalability and advanced capabilities for managing traffic and systems. Integrating load balancing across several data centre's is essential for preserving web application security and guaranteeing uninterrupted service functioning, especially during periods of high client demand. This method enhances high availability by redirecting traffic away from unavailable resources and enables system monitoring and administration, including health checks and managing simultaneous connections. As organizations increase their online presence, it becomes crucial to have efficient load balancing servers, strong application firewalls, and Cloudflare load balancing solutions to protect against internet attacks and offer a seamless user experience.

## Literature Survey

Load balancing is crucial in cloud computing settings to provide uninterrupted service and successfully fulfill user expectations, given the growing complexity and requirements. An extensive overview of the existing literature on load balancing techniques for virtual machines (VMs) was given at the 2020 International Conference on Innovative Computing & Communications (ICICC). Load balancing evenly distributes workloads among all nodes, resulting in reduced execution time, minimized communication delays, and maximized resource efficiency and throughput. The study examines several load balancing techniques, including static, dynamic, and hybrid approaches. The authors have conducted a comparative analysis of approaches such as FIFO and LIFO, with a specific emphasis on measures such as Queueing Length, CPU Utilization, and Power Consumption. An innovative load balancing approach was presented, using clustering to allocate jobs across cooperating nodes, resulting in notable improvements in resource management as shown by simulation outcomes. This clustering methodology not only improves the effectiveness of load distribution but also leads to energy conservation and enhanced overall system performance.

## Proposed methodology

In particular, load balancing is an essential component of contemporary security architectures for hybrid cloud and cloud computing environments. By preventing individual servers from becoming bottlenecks, it improves the resilience and security of the system. By distributing incoming traffic across numerous servers, load balancers reduce the attack surface and make it more difficult for adversaries to deplete resources. The implementation of load balancers in public cloud environments and data centers facilitates the streamlining of security protocols and management processes, ensuring a uniform security stance across all platforms. Load balancers serve as an initial barrier against Distributed Denial of Service (DDoS) assaults by

rerouting traffic intelligently in response to the detection of a potential vulnerability or threat. In response to the increasing prevalence of hybrid cloud environments, load balancing and Application Delivery Controllers (ADCs) are given priority by 57% of IT organizations in order to fulfill the requirements of these intricate architectures. It is critical to update load-balancing infrastructure in order to accommodate the dynamic and scalable characteristics of cloud-native applications and services.

## Securing Multi-Data Center Architecture

Effective data sharing and security across physical areas are made possible by load balancing, which is an important part of the security design of multi-data center settings. Distributed Denial of Service (DDoS) attacks are one type of attack that this is not enough to protect itself from. By redirecting traffic away from computers that look like they could be attacked, load balancers add an extra layer of security to multi-data center protection. In the event that some parts of the network are hacked, this function keeps service and security up and running. It is known by 89% of IT teams that load balancers are an important part of their company's total security system. If you want to make load balancers work better and lower the risks of DDoS attacks, you should definitely use a full defense plan that includes multiple safety methods at different network points. As a result, the network infrastructure is much safer across various data centers, and it is also much more available and faster.

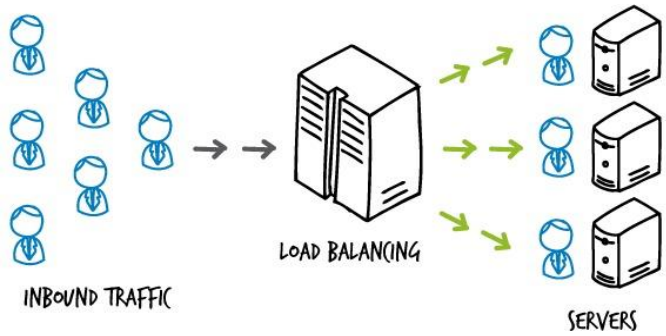


**Fig. 1 Architecture Diagram**

***Use Case Diagram:***

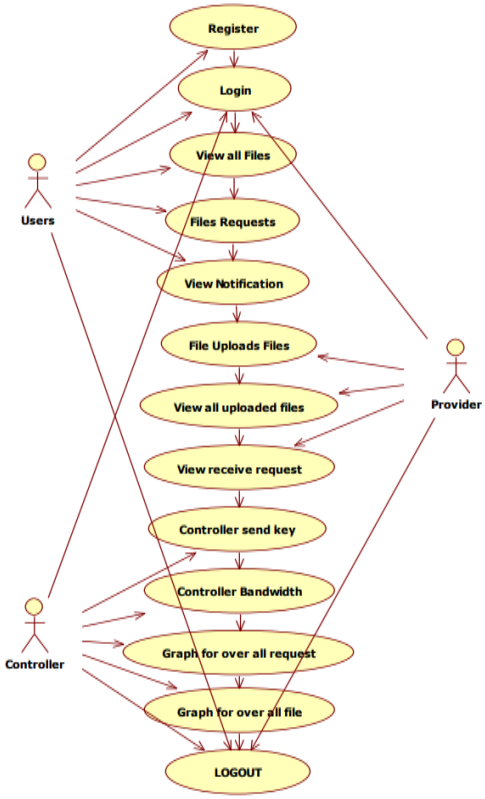


**Fig. 2 Use Case Diagram**

***Sequence Diagram:***

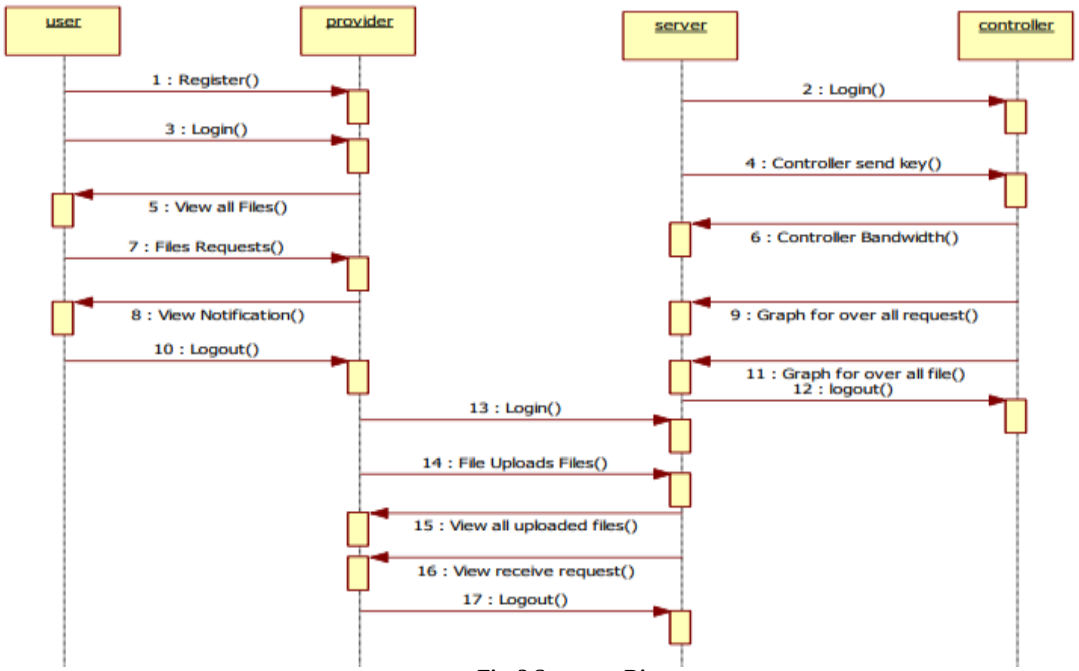


**Fig. 3 Sequence Diagram**

***Understanding Load Balancing in Multi-Data Centre Configurations:***

Distributing server workloads uniformly across several data centres is the goal of load balancing, which is also known as global server load balancing (GSLB). This approach improves speed by reducing the likelihood of server overload and reliability by allowing for failover in the event of server failure. GSLB ensures service continuity and minimizes downtime by automatically redirecting traffic away from servers that are experiencing trouble to ones that are fully functioning. Each data center runs autonomously with its own set of Access Manager installations in such settings, enabling localized resource control within a larger architecture. The OAMAuthn cookie improves session stickiness and user data affinity across sessions started in separate data centers, making session management in multi-data center deployments complicated. Active-Active, Active-Passive, and Active-Hot Standby are some of the topologies used to manage systems and distribute traffic in settings with several data centres. Global organizations that need high availability and low reaction times across diverse geographic locations might benefit from Active-Active configurations because they optimize resource usage and offer the maximum degree of redundancy and availability.

***How to Implement Load Balancing Across Multiple Data Centers***

Load balancing across various data centers needs a strategy plan that includes both hardware and software options. The BIG-IP Global Traffic Manager (GTM) and BIG-IP Local Traffic Manager (LTM) are very important for handling user requests correctly based on where they are located. To setup, set up trust relationships between BIG-IP devices, make the appropriate parts, set up the GTM pool and Wide IP, customize DNS settings, and set up DNS clients. Devices in different data centers need to be able to trust each other in order to work together without any problems. Within the BIG-IP system, data centers and server objects should be set up, and the GTM pool and Wide IP should be set up to handle traffic well. To set up DNS settings, you need to add BIGIP-02 to the sync group, make sure both devices are set to GTM sync, and add DNS names.

***Testing and Validation:***

It is suggested that checking access with tools like PING and Horizon be done to make sure the system is working correctly. This helps to make sure that the GTM is working right in both Site A and Site B, making sure that traffic is fair and that service 12 isn't interrupted. By following these specific steps, businesses can make sure that their load balancing setup across various data centers is strong, effective, and able to handle the high volume of network traffic today. This method not only improves the speed of applications, but it also makes the system more reliable by reducing the number of possible breakdown places in the network infrastructure.

***Key Considerations for Implementing Load Balancers:***

To effectively manage the flow of traffic between users and web servers, load balancers are an essential tool. It is possible for them to be based on either hardware or software, with hardware referring to actual devices and software referring to virtual solutions. For both, careful setup is required on

each individual server. The choice of load balancing method is determined by parameters such as the magnitude of the workload, the resources that are available, and the quality of the solution that is required. This option is influenced by a number of factors, including round-robin, the number of connections, the IP hash, and the load on the server. It is possible to provide a safe manner between data centers and public clouds by integrating load balancers into hybrid cloud and application delivery controller (ADC) systems. Through the use of load balancers that are positioned behind network firewalls, vital business systems may be protected from possible attacks.

***Balancing Strategies for Multi-Data Center Deployment:***

For best performance and high availability, load balancing solutions are a must for handling network traffic across several data centres. To avoid any one backend server from being overloaded, high-performance load balancers distribute incoming traffic equally across all of them. Integrating load balancing with other network and security technologies, such intrusion detection systems and firewalls, is essential for multi-data centre deployments to provide a complete network security solution. By using a software-defined technique, DNS load balancing guarantees that DNS queries are sent evenly across servers. In order to manage high amounts of traffic, servers with hardware load balancers safely route the traffic to several servers, while servers with software load balancers loaded on them perform the same duties. The effective management of network demands and the maintenance of system performance in dispersed environments are made possible by both types, which are essential for redirecting requests to particular virtual instances.

***Case Studies and Real-World Applications:***

Load balancing across several data centers is an essential technique in numerous practical applications. For example, a prominent e-commerce business used load balancing techniques to handle web traffic during busy shopping periods, guaranteeing excellent availability and strong performance. In order to improve data security and operational efficiency, a worldwide financial services company used load balancing techniques. They achieved this by using both hardware and software load balancers to govern the flow of traffic and safeguard valuable financial information. A prominent hospital network in the healthcare industry used load balancing technology to optimize the administration of patient data across many locations, guaranteeing immediate access to crucial patient information. The load balancers efficiently managed data requests during moments of high demand, such as medical crises, therefore improving the responsiveness and dependability of the hospital's IT infrastructure.

## result analysis

In load balancing across various data centers, Oracle Access Management (OAM) and Oracle Identity Manager (OIM) inside the Oracle Identity Governance (OIG) architecture have shown great success. Multi-site systems improve security and performance across geographically distributed data centers 16. Active-passive or active-active deployment strategies allow OIM to easily adjust to network delays, guaranteeing robust data processing and user authentication 16.

The Global Load Balancer (GLBR) and Local Load Balancer (LBR) ensure system continuity and performance. In case of site failure, the GLBR redirects traffic to functioning sites using pre-configured criteria such the client's geographical IP and a pool of local load balancer addresses 16. Persistence mechanisms like Active Insert of a cookie are essential for client session affinity and traffic routing across many data centers in the LBR. 16.

Using Apache Jmeter, the round-robin method surpassed the least connections strategy in CPU usage and queue length 17. Open-source PHP, HAProxy, MariaDB, and Cloud Firewall were used to develop a secure multi-data center architecture on Digital Ocean 17. These findings emphasize the necessity of load balancing methods and setups for multi-data center performance and security.

## Conclusion

During the course of this investigation into load balancing across numerous data centers, we have consistently emphasized the critical significance of this technology in bolstering security, assuring peak availability, and optimizing performance in distributed computing environments. Through an examination of diverse load balancing strategies, encompassing both hardware and software solutions as well as dynamic and static methodologies, we have established the manner in which distributed traffic not only maximizes the utilization of resources but also safeguards the integrity of the system against potential cyber threats. The importance of integrating advanced load balancing mechanisms cannot be exaggerated, particularly in the current era characterized by the criticality of digital transactions and data security, as demonstrated by practical implementations in various industries including retail, financial services, and healthcare.

Furthermore, the discourse pertaining to the implementation of load balancing technologies, encompassing the factors to be taken into account when selecting algorithms and integrating them with other network security measures, emphasizes the careful strategizing that is necessary to ensure security and optimize processes in configurations involving multiple data centers. The ramifications of these technologies extend beyond simple traffic management and affect crucial facets of operational efficiency, data integrity, and system resilience. In light of the intricate nature of contemporary network infrastructure, the knowledge and understandings presented here establish a fundamental basis for the deployment of resilient, effective, and protected load balancing mechanisms that accommodate the ever-changing requirements of worldwide digital ecosystems.

REFERENCE:

[1] https://www.linode.com/docs/guides/load-balancing-fundamentals/

[2]https://www.researchgate.net/publication/325210659_Secure_and_Sustainable_Load_Balancing_of_Edge_Data_Centers_in_Fog_Computing
[3]https://www.irjmets.com/uploadedfiles/paper//issue_9_september_2022/30303/final/fin_irjmets1664454959.pdf
[4]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10702718/
[5]https://link.springer.com/10.1007/978-3-319-32903-1_325-1
[6]https://kemptechnologies.com/load-balancer/load-balancing-algorithms-techniques
[7] https://avinetworks.com/what-is-load-balancing/
[8]https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html
[9]https://sre.google/sre-book/load-balancing-datacenter/
[10]https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3564355_code3635775.pdf?abstractid=3564355&mirid=1
[11]https://www.researchgate.net/publication/319101865_A_literature_review_on_algorithms_for_the_load_balancing_in_cloud_computing_environments_and_their_future_trends
[12]https://avinetworks.com/glossary/multi-site-load-balancing/
[13]https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/understanding-multi-data-centers.html
[14]https://www.techtarget.com/searchnetworking/definition/load-balancing
[15]https://www.edgenexus.io/blog/6-things-to-consider-when-deploying-load-balancer/
[16]https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/imedg/multi-data-center-deployment.html
[17]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7767358/
[18] https://hongzhangblaze.github.io/assets/pdf/Hermes.pdf