International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 13, Issue 4 (Jul.-Aug. 2024), PP. 10-15

An Enhanced Load Balancing Methodology in Distributed System Environment

Dr. K.KUNGUMARAJ
Associate Professor, School of Applied Science, Sapthagiri NPS University, Bengaluru.

ABSTRACT: *At present, there is a massive usage of internet sources with the implication of distributed system architectures. Information exchange with several web applications requires security methods. In particular, sensitive data faces the risk of security threats. Cryptography combined with a biometric feature is an enhanced security mechanism developed to resolve it. When much loads of data are in a communication network causes the overhead of adaptability, accessibility, and imbalance in load distribution. Traditional load balancing in clustered web servers are limited in faster response times, and greater performance.*
Keywords: *Load Balancing, Cluster server, Information exchange.*

Date of Submission: 20-07-2024 Date of acceptance: 03-08-2024

I. INTRODUCTION

A network is an assembly of two or many more devices that can communicate. These devices may be computers, servers, mainframes, or peripherals that allow sharing data. Network connections may be physical or wireless. Networks are of distinct types and are classified based on their respective characteristics, like connection types, wired or wireless-architecture, and their topology. The distinctive types of networks include local area networks, wide area networks, metropolitan area networks, and backbone networks. Distributed computing environments have become an economical and prominent option to acquire high performance and to rectify wide-ranging computational complications. Generally, the distributed system is referred to as a gathering of autonomous computers that are interconnected along with a network, and their activities are coordinated through distributed middleware and they share the system resources simultaneously. From the users' point of view, it is treated as a single system, combined with calculating ability.

The main focus of using a distributed approach is sharing resources. During every processor cycle period, the main resources are shareable. This redistribution of the load is done by the distributed system which is one-off the components in a distributed operating system and resource management resulting in optimizing the performance of the entire system. Figure-1 shows the Distributed System Architecture. The key features of the distributed framework are:

- It allows the sharing of resources, interconnected network software systems that are done simultaneously.
- It supports multiple components, but they are independent.
- There will be greater fault tolerance in this system when compared to other network models.
- The cost of backhauling capacity utilization is reduced.
- Latency is lowered; the probability of smooth communication is increased due to an endpoint to endpoint delay reduction.

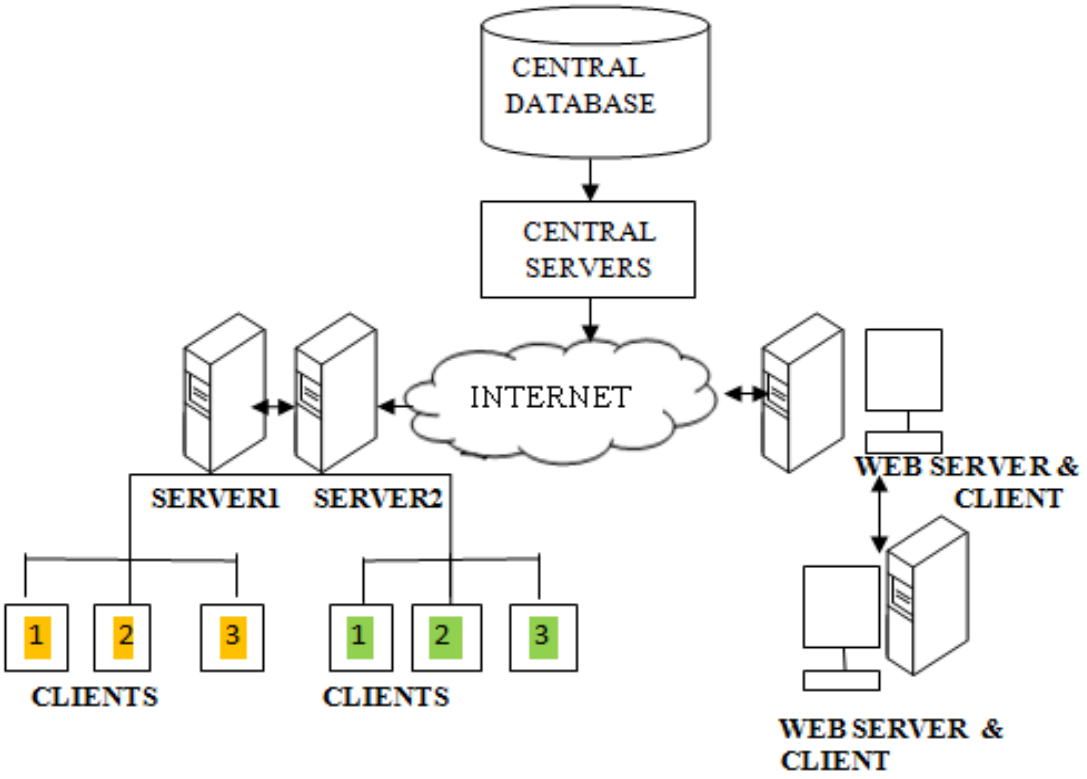

Figure-1: Distributed System Architecture

II. DISTRIBUTED SYSTEM CHARACTERISTICS

Today distributed system is everywhere since it provides high performance and computation power to serve the increasing need for large applications. The following are the characteristics of a distributed system:

Large Scale: The potential of a distributed system to accommodate more users without affecting the performance metric is called scalability. It can be attained by appending more nodes with fast processors. As the count of nodes increases, components of the system shouldn't require any change.

Geographical Distribution: The servicing systems of the distributed system may be located in distant places.

Heterogeneity: The host which has both software and hardware resource sharing based on the range of files, data, display devices, supercomputers, and PDA's.

Resource Sharing: Distributed system based computers can use any hardware or software at any location. Resource manager controls the resource access, resource concurrency and it performs a mapping scheme. The sharing model may be either object or client-server based. These models reveal how resources are shared, used, and interact with users and resources within themselves.

Transparent Access: The distributed system will work in a transparent way which makes the distributed model be viewed as a single virtual computer from the user's perspective.

Quality of Service (QoS) Requirements: The quality of the distributed system must be sustained, predictable and assures the basic quality of service.

Consistent Access: Standard devices must be used for building distributed systems like interfaces, protocols, and services. So that it hides the resource heterogeneity while permitting its scalability. Failing to produce such standardized services, then the application can not be possible to function properly.

Pervasive Access: With the option of a dynamic environment the distrusted system must provide an accessing facility to the available resources even in case of failures.

Openness: In distributed system improvements and extensions are concerned with openness. Numerous frameworks of distributed systems are associated with each other over interfaces, so all these interface information is published in detail. Any new component further added to the system must be combined with prevailing components. Owing to varied components, the problem of dissimilar data illustration structures rises which have to be determined.

III. ISSUES IN DISTRIBUTED SYSTEMS

The objective of distributed computing is to integrate resources spanning more organization into virtual ones which can solve significant problems in engineering, business, scientific applications more effectively. To attain this objective the subsequent problems must be taken under consideration as follows:

Transparency: One of the important goals of the distributed model is to create an invisible outlook of multiple computers to a single image to user visibility.

Reliability: It refers to the fault tolerance mechanism which results in higher reliability on distributed systems while comparing with a centralized system. Because in distributed systems multiple instances of resources are available, even if there's a fault that occurred it can be overcome by recovering it with other resources.

Scalability: It refers to adapting an immense number of service loads with the appropriate capability of a distributed system. It is unavoidable in a shared environment that has growing machines or hosts, even a small work added increases the workload. Thus, a distributed model must be designed to easily handle the growth of users and nodes' to maintain an inappropriate loss of performance.

Heterogeneity: It is very difficult to design a distributed system that is heterogeneous, which comprised of different hardware or software systems interconnected.

Security: Imposing security in a shared (distributed) system is very difficult compared to a centralized system because they lack in single-point control. [8] Thus, it is necessary to protect various resources available in the distributed system and the possibility of destruction and unauthorized access and has to be avoided.

IV. TYPES OF ATTACKS ON INFORMATION IN DISTRIBUTED SYSTEMS

In communication, information is the most vital aspect. There are wide varieties of attacks on Information processing. They are,

Brute Force Attack: This attack is like a trial and error method. It is wont to obtain sensitive information like password personal identification numbers. This attack is applied by generating a larger number of guesses until the desired information is got. All this can be done by automated software. These attacks shall be used by cybercriminals to crack sensitive data. Security analysts also use brute force attacks to evaluate the strengths of security levels on data. This attack is the most time consuming and resources consuming. The success rate of this type of attack is based on computation power and the count of attempts tried to crack the desired data.

Collusion Attacks: A secret agreement is made with an opponent by a node to leak information. Once a node is correlated to the opponent node, the adversary collects all the confidential information as desired. Once the desired information is collected from the system, attacks are made by manipulating with wrong data injection through compromised nodes.

SQL Injection Attacks: SQL Injection attacks are made for backend database manipulation. Some information may not be displayed on the front end. This information may include sensitive data about an organization or customer details. To get access to this backend data attacker implies malicious SQL code in terms of queries.

Dictionary Attacks: Dictionary attacks are a type of brute force attack. It is a scheme of tracing sensitive data such as passwords, attempting to find the key for encoding and decoding messages, or a document by systematically entering the word in the dictionary. These attempts work because many use normal words as passwords. There are some unsuccessful cases when a combination of uppercase and lowercase, or digits mixed in the passwords or keys. These attacks can be avoided by limiting the attempts to access within a short period. For example, while entering a PIN in ATM only three attempts are allowed. If the wrong PIN is entered card will be blocked. The same is the case when passwords are entered for opening mail or other online bank transactions.

Side-Channel Attacks: Side-channel attacks depend on working or analyzing what a computing device does when attempting to perform cryptographic operations. Side-channel attacks monitor the computer's consumption of power and electromagnetic emissions. By reverse engineering process security tokens are generated. Other techniques of side-channel attacks are cache attacks, timing attacks.

Man in Middle Attack: This attack happens on public-key cryptosystems. Before the beginning of communication, there exists a key transfer. Many algorithms suffer from this attack. Suppose consider,

- Host "L" communicates to Host "M", hence requests the public key of "M".
- The Attacker sends the public key and obstructs the request.
- The attacker will be allowed to read whatever data send by host "L" sends to "M".
- To extend communication, the attacker re-encrypts the data after reading with his key (public) and dispatches it to "M".
- "M," thinks that it is getting data from "L" instead it is from the attacker.

V. NEED FOR SECURITY IN A DISTRIBUTED COMPUTER SYSTEMS

Due to the increased utility of the internet in this network era during the data transmission, there is an explosion of information, and users have started growing tremendously and it becomes a very important and unavoidable activity in human life. There arises the need for protecting the data while in transmission and performing verification and validation process of the data and send it for the authenticity of the sender and receiver. The acceptance control mechanism needs the authentication base process for accessing the resources by the users by providing such a secured network it is assured that only the intended receiver can interact. In the conversion, can read the message addressed to him/her. There are possible violations that compromise the secrecy of the transaction. Hence protecting secret information becomes compulsory. Secrecy is negotiated when the secret information is divulged to users not endorsed to reveal it.

VI. RESEARCH MOTIVATION

The main motivations of the server load balancing are,

- Achieve optimal Resource Utilization
- Maximize the throughput
- Minimize the response time
- Avoid overload
- Avoid crashing

VII. RESEARCH METHODOLOGY

In load balancing scheme security is another important issue in the aspect of a distributed system. Thus, SSL load balancer is involved in encryption/decryption of data using HTTPS which utilizes Secure Socket Layer (SSL) protocol to provide security on the system. The load adjuster receives the incoming request of clients and distributes them among clustered servers and thus it increases the reliability, scalability, and performance of the entire system. TLS session sharing can be carried out to achieve load balancing. The TLS and SSL are the conventional protocols for encrypting the data before it is transferred to the network, which protects it from unauthorized access performed by third parties. It is important for preserving confidential data like security related numbers, credit-card details during transmission over the network.

The SSL load balancer behaves like a server-side SSL reach point for interconnection with clients, it performs both cipher and deciphering of requests and responses. The process involved in the security scheme varies relying on the load balancer and the server.

- If the server and load balance are in the same firewall then the SSL load balancer will involve in the decryption of request and pass it to the server as plain information. At the equivalent time, the response sent by the server is encrypted and forwarded to the client.
- In case if the network among load balancer and server is not secured then the SSL load balancer is structured such that after the request from the user is received by SSL, it decrypts the needed information and re-encrypt the request before passing it to the main server. The process is reversed for the process of responding from the server to the client.

Performing the encrypting and decrypting process is done offload will intensively permits web and application servers and increase the process of content delivery and increases the overall user expectations as needed. Suppose if the load balancer and server work is a secure network then install and manage security using SSL certificates on load balancer rather than on web and application server. This primarily reduces the administrative overload if the group of servers is high.

VIII. RESULTS AND DISCUSSION

The result below shows that to reduce packet drop, to improve throughput rate and reduce latency in a distributed computer systems. To calculate the drop rate first got to determine the number of packets dropped. Number of packets dropped can be found out with the formula,

Number of packets dropped=Number of packets sent- Number of packets received

Drop rate %= (Packets dropped/ Packets sent)*100.

In real time scenario,

Number of Packets sent = 34455

Number of Packets received=24808

Number of Packets Dropped=9647

Packets drop-in (%) =28 %

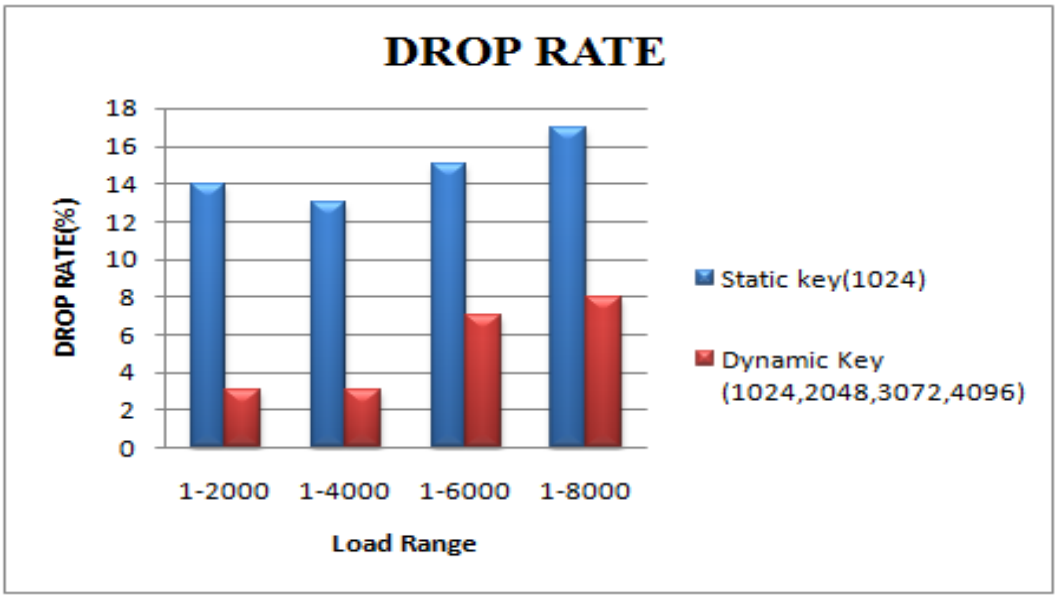

Figure-2: Packet Drop Rate

Figure-2 shows the Packet drop rate in a distributed computer systems. The processing of client requests by Server1 in graphical results is shown in the below Figure- 3 and Figure-4.

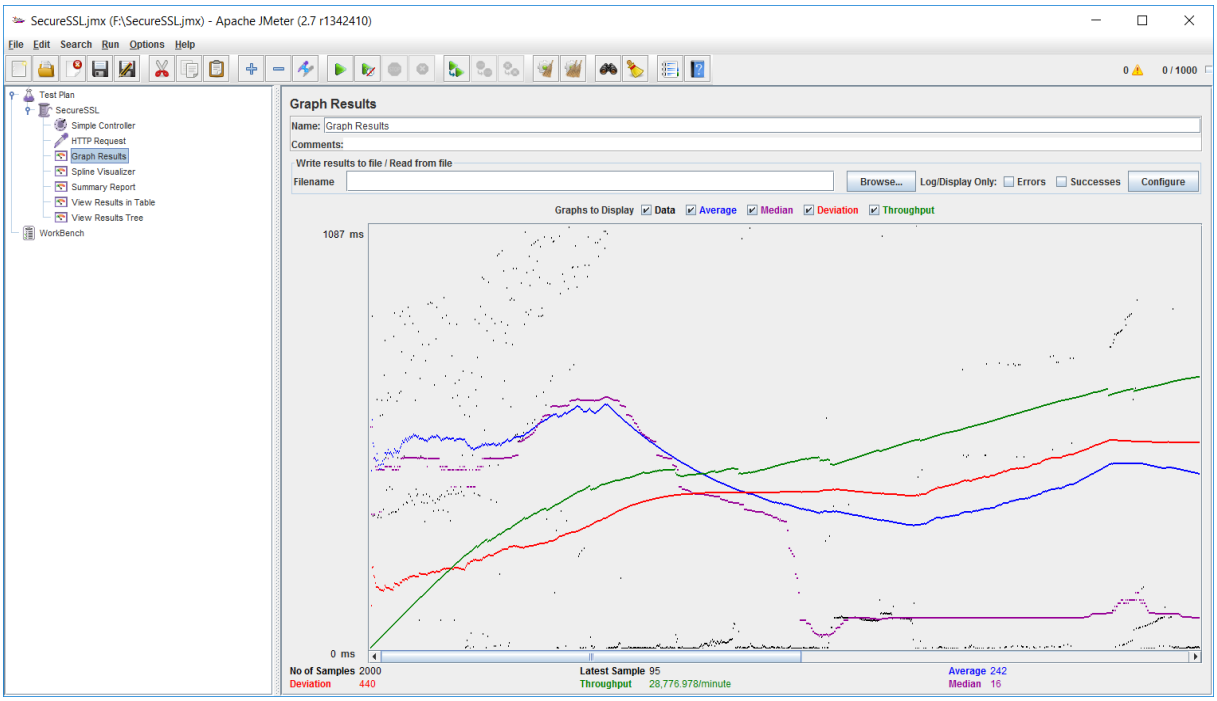

Figure-3: Server1 client requests processing

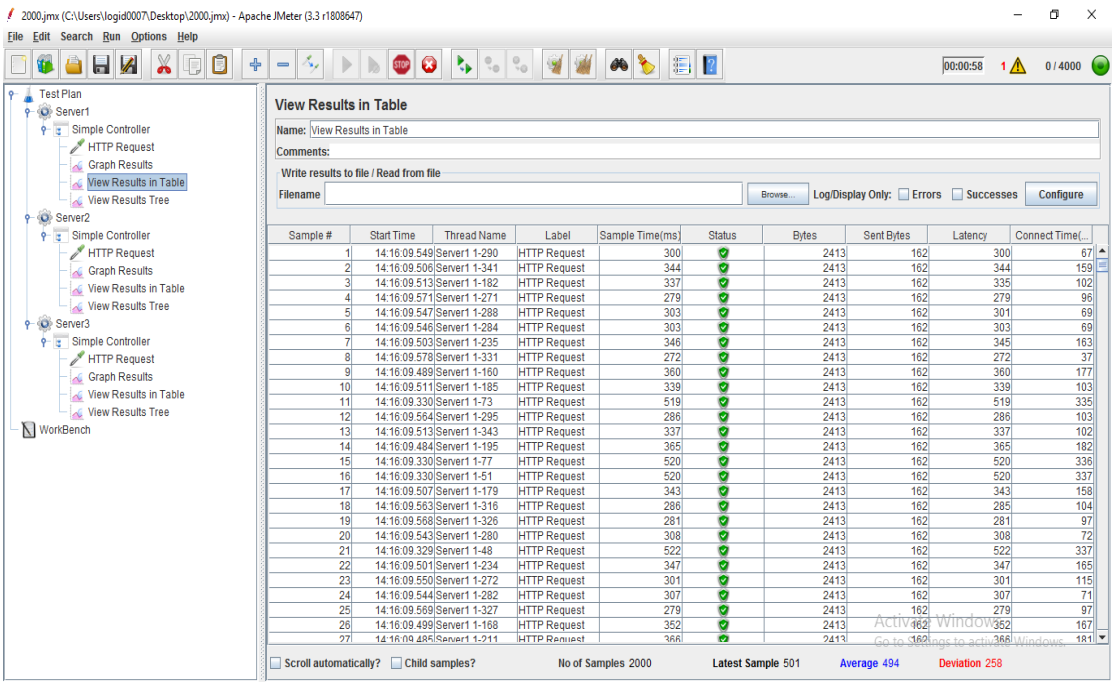

Figure-4: Set of client requests processed by server1

Main server calculates the work load for the first server, second server, and third server and so on. Based on the less loaded server, new client request can be allocated to the particular sub server.

IX. CONCLUSION

The primary objective of this thesis work is to handle the load distribution among the web servers in a secure manner. The usage of web applications and their services, heterogeneous web server clusters are interconnected through the network and they are involved in intercommunication among hosts and end-users with satisfied cost-effective methods. This research involves not only load balancing, but during data transmission, among the heterogeneous distributed environment the confidentiality of the data is also preserved by developing a mechanism.

REFERENCES

[1]. Akshay Daryapurkar , Mrs. V.M. Deshmukh, 2013, "Efficient Load Balancing Algorithm in Cloud Environment", International Journal Of Computer Science And Applications, Vol. 6, No.2, pp.308-312.

[2]. Deepti Sharma, Dr. Vijay B. Aggarwal, 2016, "Improving Performance of Dynamic Load Balancing among Web Servers by Using Number of Effective Parameters", International Journal Information Technology and Computer Science, pp. 27-38.

[3]. Dhurandher .S.K, M. S. Obaidat, I. Woungang, P. Agarwal, A. Gupta and P. Gupta, 2014, "A cluster-based load balancing algorithm in cloud computing", IEEE International Conference on Communications (ICC), Sydney, pp. 2921-2925.

[4]. Mostafa Samih & Rida, S. & Hamad, Safwat., 2010. "Finding Time Quantum Of Round Robin Cpu Scheduling Algorithm In General Computing Systems Using Integer Programming", International Journal of Research and Reviews in Applied Sciences, pp.64-71.

[5]. Punit Gupta, Mayank Kumar Goyal, and Nikhil Gupta,2015, "Reliability Aware Load Balancing Algorithm for Content Delivery Network", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI), Volume 1, pp.427-434.

[6]. Xu Jinhong & Yang Xiaoguang., 2017, "Research on key technologies of technological service and management based on cluster load balancing", Cluster Computing, pp. 3409-3415.

[7]. Zhu X.M. and Lu P.Z., 2009. "Multi-dimensional scheduling for real-time tasks on heterogeneous clusters". Journal of Computer Science and Technology, 24(3), pp.434-446.