Security Approaches and Load Balancing Methodologyin Clustered Web Servers

[1]Dr.K.KUNGUMARAJ

[1]Assistant Professor in Computer Science, Arulmigu Palaniandavar Arts College For Women, Palani

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. With an intruder act in the network causes security breaches despite using various security providing algorithms. Though there exist security algorithms like RSA, AES, DES, etc., many vulnerabilities occur due to static/dynamic key usage. Attacks like brute force, collusion, SQL Injection are some of those which keep data in a vulnerable state. Key generation is the primary concept in these algorithms, and when the key can be achieved through trials, it is much more vulnerable. The performance of the security algorithm depends on the key size. Computation and time complexity increases when the key size is large. Cryptography combined with a biometric feature is an enhanced security mechanism developed in this research work. A random 512-bit secret key is generated from the ear feature in the developed methodology.

Keywords: Load Balancing, Secret Key, Distributed system, Cluster web server

1. 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. The network is created for communication and can proceed only if it follows some protocol. That protocol is TCP/IP. A switch in this context is a speedy device that accepts incoming data packets and ensures them to reach the destination by redirecting the packets.When more numbers of systems are interconnected more communication between systems takes place. As the prevalence of the Internet growing rapidly the working capacity of network servers is predicted that it becomes a bottleneck in organizing network-based services. Other prominent problems are cyber-attacks and security breaches that cause major issues and impact the development.

2. ISSUES IN DISTRIBUTED SYSTEM

The objective of distributed computing is to integrate resources spanning more 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. Whereas the homogeneous system consists of closely related or the same features of hardware and software.

Security: Imposing security in a shared (distributed) system is very difficult compared to a centralized system because they lack in single-point control. (Antonio Mana et al. 2012) 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.

3. NEED FOR SECURITY IN DIFFERENT ASPECTS

Security is needed in three different aspects. First is the security of information, avoiding unauthorized access, and loss of data. Second is the computer security, to protect private data from hackers. And third is Network security. Security is not limited to one network but a network of networks. Important information in large amounts is exchanged in any unspecified network of an organization. This information must not be accessed by the attacker and misused. Here are some reasons for information security:

- To protect the data from undesirable altering, accidentally, or purposefully by unapproved clients.
- To shield the data from loss and make it to be conveyed to its destination appropriately.
- To manage and to acknowledge the message received by any node to protect from the denial by the sender in a particular situation.
- To restrict a client to send a message to another client with the name of a third one.

- To safeguard the message from an undesirable postponement in the transmission lines or routes to convey it to the required destination in time, in case of emergency.
- The information is transferred as data packets form. To protect the packet data that wait for an elongated time leading to traffic blockage in the network route where the destination system unable to capture the packet because of internal faults.

The second part of security is computer security. Every computer is vulnerable to various attacks. It is the primary responsibility of the user to protect it from attacks. Every individual system must be pre interpreted with some security measures to shield from hacking, viruses, and worms, spyware, adware, etc. If any such attack occurs hard disk data will be completely wiped off and result in hardware problems too. Computers and networks must be protected from damaging software. Computers are part of the network so securing personal computers from hackers is a necessary task. Need for Computer security is due to the following reasons:

- Protecting from replication and capture viruses from affected files.
- Protecting from malware, webworms, internet security threats, and bombs.
- Providing a Firewall software security mechanism from unauthorized access.
- Protecting from Trojan Horses as they are dangerous to computers.

The third is the network security deal with security problems in a network and other network applications. (Jameela Al-Jaroodi et al. 2010) Network security is for the following reasons:

- Protecting a computer network is the significant responsibility of the person who takes care of securing the network.
- The network must be protected from unauthorized entry into the network, usage of unwanted malware, and internet threats.
- Unauthorized entry into the network causes network traffic by sending duplicate packets of data.

4. STATEMENT OF THE PROBLEM

This research work aims to define the existing problems in the area of clustered web servers as follows:

- The existing load balancing mechanism fails to handle the security breach when both the load-balancer and server are not in a secure network.
- Though both load balancers and servers are in a secured network with the use of SSL digital certificates if they transfer information, then there is a high possibility of spoofing as a normal user by the intruders and try to break the confidentiality and authenticity of the distributed system.

- While using static keys for encryption/decryption purposes, during information transmission among client, load balancer, and web server, there is a high degree of intrusion in an open network.
- While eavesdropping by intruders is achieved, then there shall be a high possibility of packet loss or a drop between client-server communications.
- The performance efficiency of the server will be degraded due to the long process of security mechanism and inappropriate unbalanced overloading on the web servers.

5. SECURITY APPROACHES AND LOAD BALANCING TECHNIQUES IN CLUSTERED WEB SERVERS

Load balancing means partitioning the work and assigning it to the available resources in an equal ratio. Load balancing can be designed with hardware, software, or a grouping of both. To adjust the load among servers evenly the clustering servers are initiated. The web servers are clustered due to its heterogeneity behavior like programming languages, mismatch of hardware, database schema, operating platforms, and topology. In many cases, the specific server in the clusters overloaded. To reduce such issue load balancing technique is introduced which obtained the perfect server for the request from the group. In this approach SSL based load balancing technique is used. In this series of developments, the server load is calculated by the server itself through the information presented in the SSL.The main intent of the research is to estimate the load and distribute the load amongst the servers. Existing load balancing methods like SSL_Session, Round robin, and SSL_Backendforwarding reduces the payload of the server. Round robin does not acknowledge priorities. The expiry of the session occurs in a short duration of time, which leads to packet loss. According to SSL backend forwarding uses an intelligent load balancing scheme but uses a static RSA scheme which creates security overhead. To overcome the issues in the existing algorithms a new procedure called Load balancing algorithm is developed for an efficient secured load balancing.

Our advanced SSL based Load balancing algorithm works dynamically for every HTTP request and response securely. In our previous study SSL, this operates between the HTTP and TCP network layers and is the most famous tool that delivers a secure channel amongst a client and a Web server. Especially, maximum Web servers/data centers supporting e-commerce applications deploy SSL to provide improved security to Web traffic. Data encryption, a security technique interprets data into another form, or code so that only people with access to a secret key (officially called a decryption key) or password can read it. Encrypted data is usually mentioned as cipher-text, while unencrypted information is named plaintext. Currently, encryption is a unique, greatest popular, and effective data security approaches utilized by administrations.

The Figure-1 represents the process flow of the SSL based Load balancing algorithm. In this process initially, the client will send a request to a web server. The server redirects the client request to the SSL based Load balancing protocol for verification. SSL based Load balancing algorithm is our advanced algorithm.

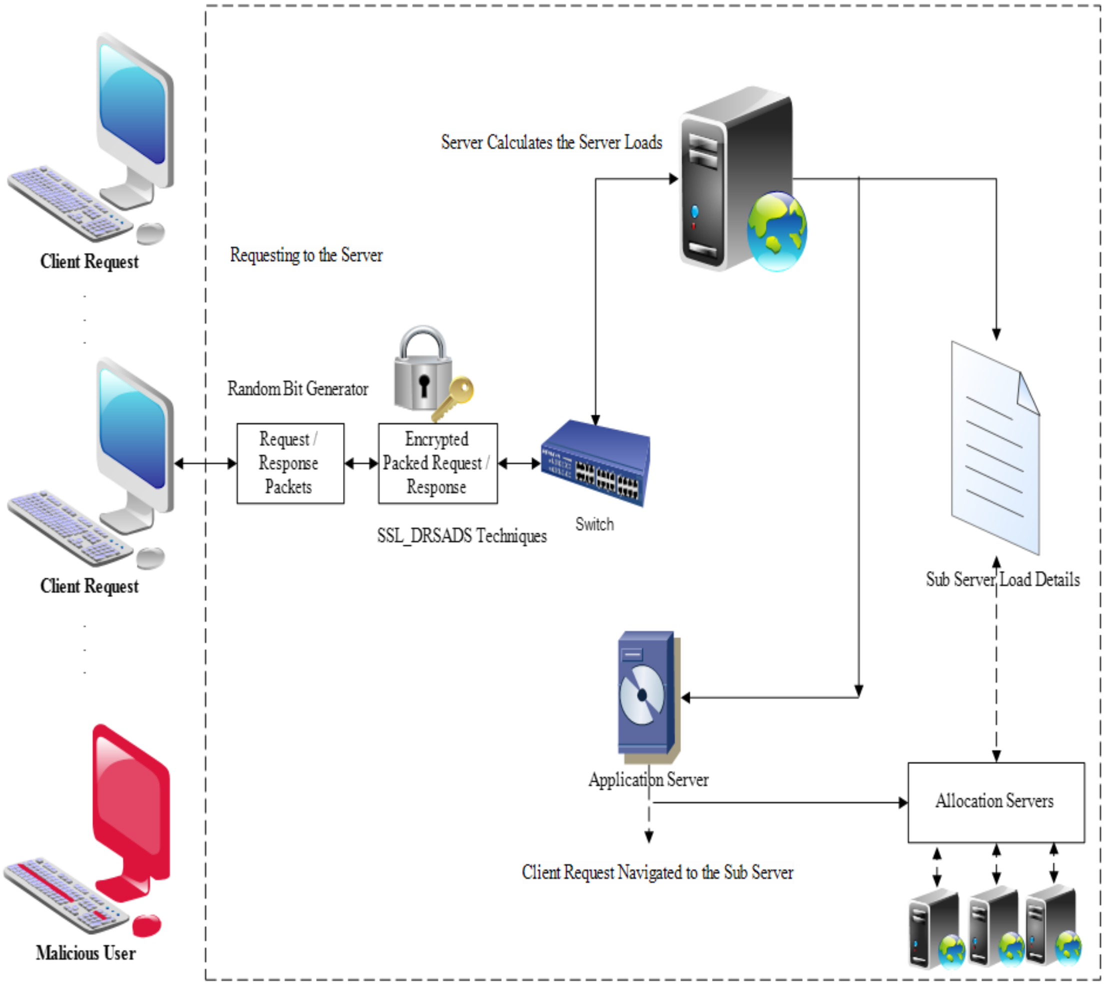


Figure - 1:Process flow of SSL_DRSADS

An SSL certificate is generated to verify the authenticity of the server. Once all the requests are encrypted all pass-through switch. This switch redirects all the encrypted requests to the application server. When an enormous number of requests are processed the server has to perform load balancing. The main server cannot process all the requests they are redirected to sub servers or proxy servers. Sub server details are to be added to the lookup table, through which the strength of sub servers can be known.

To allocate requests to the sub-servers, the application server must be known to the responding time of the sub servers. The application server sends an ECHO packet to all the sub servers. Whichever server response time is fast means that a particular server can handle the request. Based on the response time all the requests are processed. Least loaded servers will be allocated with the requests than the overloaded servers. If malicious user presents in the same network he would be able to perform many malicious attacks to theft the data. It would be easy for him to get the Internet Protocol address of other systems. But because of the usage of a dynamic encryption technique hackers cannot identify in which bit level encryption has occurred.There are at most 16 to 18 certificate authorities which issue digital certificates. These certificates explicitly specify the bit key level what they are using. Knowing that key levels intruder can apply any of the attacks such as brute force attacks, collision attacks, SQL injection, dictionary attacks, side-channel attacks, online forgery attacks, and so on. With the usage of the dynamic key, intruders' act to crack the key becomes impossible. The application server communicates a secure channel of request & response for every client request in SSL_DRSADS.The suggested system is designed to increase throughput, minimize encryption time, decryption time, latency, and balance the servers based on different workloads.

The fundamental step in the algorithm is to generate a public and private key pair. Let us consider variables k_n as public key and k_d as a private key.

k_n → public key

k_d → private key.

```
Initialize x=1;
While (x>=3)
{
$k_n = r_p * r_q$ , where $r_p$ and $r_q$ are distinct primes.
phitotient, $\varphi_t = (r_p -1) (r_q -1)$
$k_e < k_n$ such that gcd ($k_e$, $\varphi_t$) = 1
$k_d = (k_e -1)$ mod phitotient.
x++;
}
Function Random ()
{
$k_n$ =Random ($k_n1$, $k_n2$, $k_n3$)
$k_d$ =Random ($k_d1$, $k_d2$, $k_d3$)
}
```

For Encryption compute:

$$K_{cip} = k_m * k_e \bmod k_n ,\ 1< k_m < k_n.$$

For Decryption compute:

$$k_m = K_{cip} * k_d \bmod k_n.$$

Secure Socket Layer Dynamic Load Allocation Algorithm

Step 1: Check for the client requests, if available convert it into DRSADS request and then allocate it to the server.

Step 2: Continue for all the requests and check the load of the server.

Step 3: If the load of the main server exceeds then calculate the response time.

Step 4: Response time is calculated by transmitting an empty packet to all the proxy servers.

Step 5: Allocation of requests to the servers is done with the request queue allocation method.

Step 6: If the request queue is zero, then allocate a new request to the server.

Step 7: If requests exist in the queue then new requests will be in a wait state.

Random Key Generator Algorithm

Step 1: Choose bits of different sizes like 1024, 2048, 3072, and 4096.

Step 2: A random number is chosen from the above using random function.

Step 3: Generates a Digital certificate that is approved by the certificate authority authenticating the server.

Step 4: Using a random function generates a dynamic key that cannot be predictable.

Step 5: A secured request and response communication is initiated between server and client.

6. RESULTS AND DISCUSSION

The performance measure is to reduce packet drop, to improve throughput rate and reduce latency. Parameters for evaluating the performance of our research work are noted below:

(i) Packet Drop Rate Calculation:

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.

For an explanation in real terms:

Number of Packets sent = 34455

Number of Packets received=24808
Number of Packets Dropped=9647
Packets drop-in (%) =28 %

Packet drop percentage is calculated from 2000, 4000, 6000, and 8000 load numbers. The drop rate is compared with static 1024 key size algorithm is compared with dynamic (1024, 2048, 3072, and 4096) key sized algorithm is depicted in both Table-1 and graphical format is represented below.

Load Numbers	Static Key(1024) (Drop Rate)	Dynamic key(1024, 2048, 3072, 4096) (Drop Rate)
1-2000	14	3
1-4000	13	3
1-6000	15	7
1-8000	17	8

Table - 1: Packet Drop Rate Static Key vs Dynamic Key

The graphical representation as in Figure-2 depicts the drop rate between the static key and dynamic key usage.

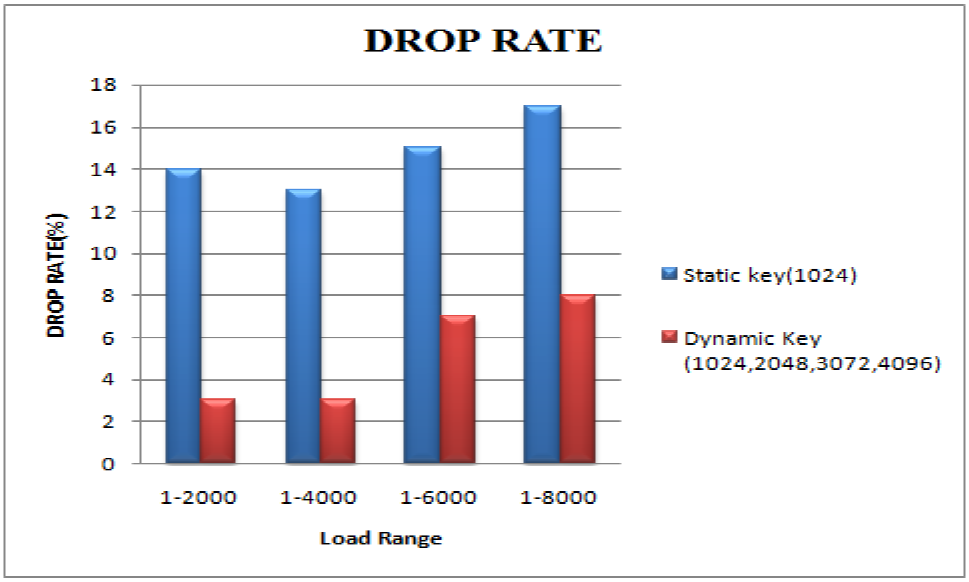


Figure - 2: Graphical representation for Packet Drop Rate

(ii) Latency Reduction rate:

Latency is another important metric. It can be calculated with the formula

Network Latency=Propagation delay + Serialization Delay

Propagation delay= Distance (between source and destination)/Speed

Serialization delay= Packet size (bits)/ Transmission Rate (bps)

Here,

(iii) Propagation delay- Is a measure in the length of time taken for a signal or quantity to proceed from the sender to the receiver. It is the time consumed to transfer bits from source to destination. Speed of propagation and distance are the two factors on which propagation delay relies on.

(iv) Serialization Delay- Is the time required by a unit of data for example say packet to be queued for transmission on a limited channel such as a cable. This withhold depends on the packet size. Lengthier packets result in longer delays in a network path. Here queuing theory is used to pass the requests. To calculate latency, we calculate the average wait time in a queue:

Latency = time taken to reach / number of checkouts

The below Table-2 depicts the comparison between various algorithms with the developed algorithm with the metric measurement latency.

Load Rate	**Algorithm**	**Latency %**
1 - 2000	SSL_LB	23
	SSL_Session	45
	Round_robin	48
	SSL_DRSADS (Proposed)	24

Table - 3: Latency Calculation

Latency is calculated for load requests of 1-2000. In contrast to existing algorithms, our developed SSL_DRSADS algorithm produces low latency. Lower latency is a good sign to get better results. But the above findings are only a limited number of requests. The graphical representation is shown in the graphical Figure-3.

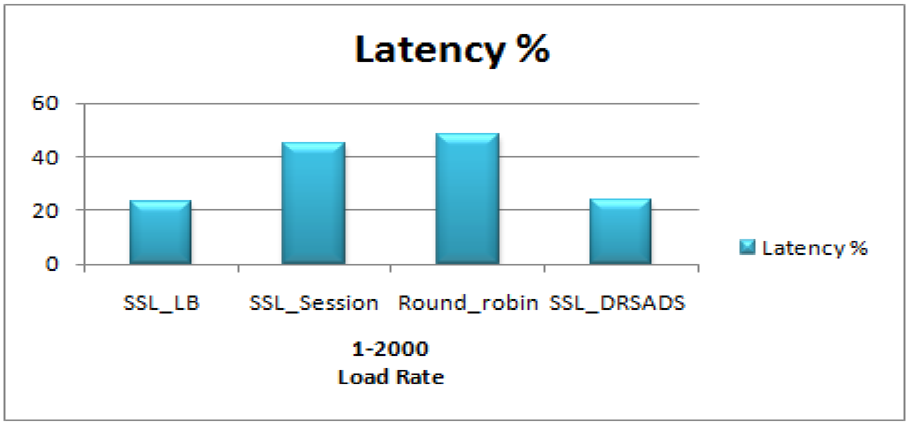
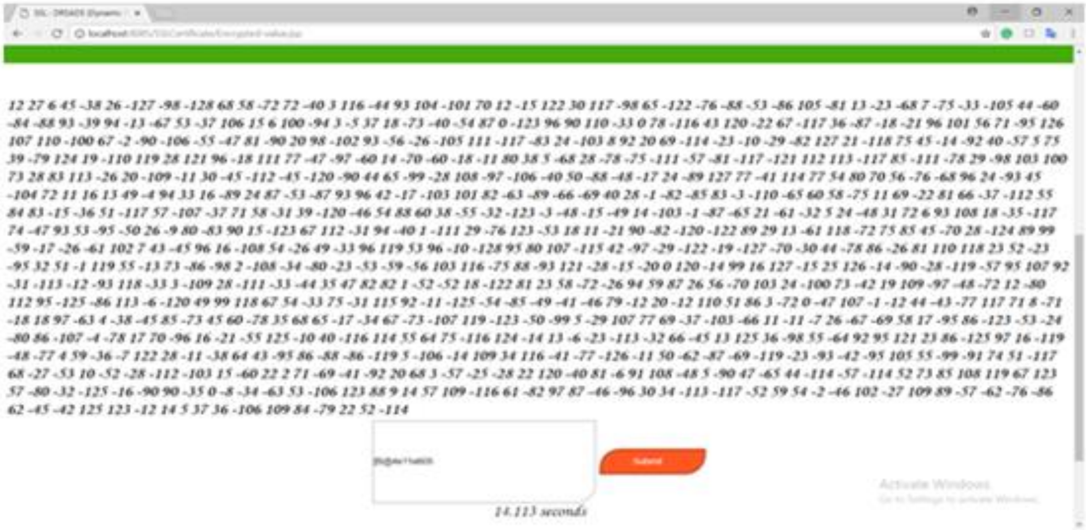


Figure - 3: Latency rate comparison with other algorithms

From the above observations, the latency is a bit high, to conquer these issues another phase development is developed and explained in the next chapter.

(v) Encryption and Decryption format:

The original message which we are sending as a request is called the plain message. When this request is passed through dynamic RSA public-key cryptosystem the message will be encrypted. If the plain message is “SSL: DRSADS(Dynamic Rivest Shamir Adleman Digital Signature) to my website”, the encrypted message of this message is shown in the below Figure-4. This may be either of 1024, 2048, 3072, or 4096 bits. The attacker cannot hack any message because the one who sent the message itself cannot able to identify in which key size it has been encrypted.

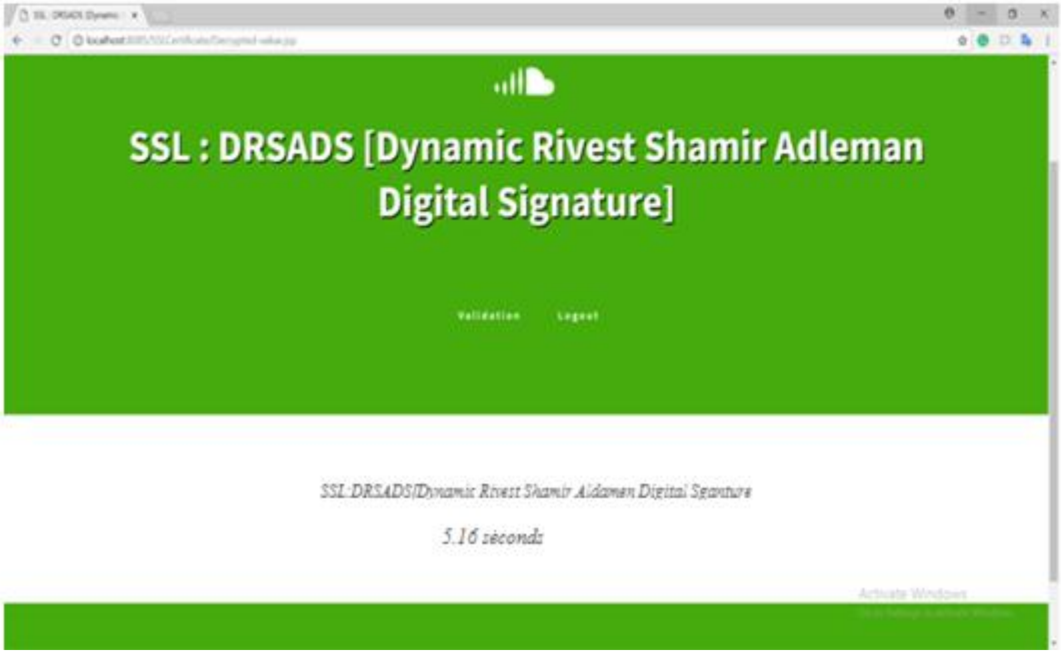


```
12 27 6 45 -38 26 -127 -98 -128 68 58 -72 72 -40 3 116 -44 93 104 -101 70 12 -15 122 30 117 -98 65 -122 -76 -88 -53 -86 105 -81 13 -23 -68 7 -75 -33 -105 44 -60
-84 -88 93 -39 94 -13 -67 53 -37 106 15 6 100 -94 3 -5 37 18 -73 -40 -54 87 0 -123 96 90 110 -33 0 78 -116 43 120 -22 67 -117 36 -87 -18 -21 96 101 56 71 -95 126
107 110 -100 67 -2 -90 -106 -55 -47 81 -90 20 98 -102 93 -56 -26 -105 111 -117 -83 24 -103 8 92 20 69 -114 -23 -10 -29 -82 127 21 -118 75 45 -14 -92 40 -57 5 75
39 -79 124 19 -110 119 28 121 96 -18 111 77 -47 -97 -60 14 -70 -60 -18 -11 80 38 5 -68 28 -78 -75 -111 -57 -81 -117 -121 112 113 -117 85 -111 -78 29 -98 103 100
73 28 83 113 -26 20 -109 -11 30 -45 -112 -45 -120 -90 44 65 -99 -28 108 -97 -106 -40 50 -88 -48 -17 24 -89 127 77 -41 114 77 54 80 70 56 -76 -68 96 24 -93 45
-104 72 11 16 13 49 -4 94 33 16 -89 24 87 -53 -87 93 96 42 -17 -103 101 82 -63 -89 -66 -69 40 28 -1 -82 -85 83 -3 -110 -65 60 58 -75 11 69 -22 81 66 -37 -112 55
84 83 -15 -36 51 -117 57 -107 -37 71 58 -31 39 -120 -46 54 88 60 38 -55 -32 -123 -3 -48 -15 -49 14 -103 -1 -87 -65 21 -61 -32 5 24 -48 31 72 6 93 108 18 -35 -117
74 -47 93 53 -95 -50 26 -9 80 -83 90 15 -123 67 112 -31 94 -40 1 -111 29 -76 123 -53 18 11 -21 90 -82 -120 -122 89 29 13 -61 118 -72 75 85 45 -70 28 -124 89 99
-59 -17 -26 -61 102 7 43 -45 96 16 -108 54 -26 49 -33 96 119 53 96 -10 -128 95 80 107 -115 42 -97 -29 -122 -19 -127 -70 -30 44 -78 86 -26 81 110 118 23 52 -23
-95 32 51 -1 119 55 -13 73 -86 -98 2 -108 -34 -80 -23 -53 -59 -56 103 116 -75 88 -93 121 -28 -15 -20 0 120 -14 99 16 127 -15 25 126 -14 -90 -28 -119 -57 95 107 92
-31 -113 -12 -93 118 -33 3 -109 28 -111 -33 -44 35 47 82 82 1 -52 -52 18 -122 81 23 58 -72 -26 94 59 87 26 56 -70 103 24 -100 73 -42 19 109 -97 -48 -72 12 -80
112 95 -125 -86 113 -6 -120 49 99 118 67 54 -33 75 -31 115 92 -11 -125 -54 -85 -49 -41 -46 79 -12 20 -12 110 51 86 3 -72 0 -47 107 -1 -12 44 -43 -77 117 71 8 -71
-18 18 97 -63 4 -38 -45 85 -73 45 60 -78 35 68 65 -17 -34 67 -73 -107 119 -123 -50 -99 5 -29 107 77 69 -37 -103 -66 11 -11 -7 26 -67 -69 58 17 -95 86 -123 -53 -24
-80 86 -107 -4 -78 17 70 -96 16 -21 -55 125 -10 40 -116 114 55 64 75 -116 124 -14 13 -6 -23 -113 -32 66 -45 13 125 36 -98 55 -64 92 95 121 23 86 -125 97 16 -119
-48 -77 4 59 -36 -7 122 28 -11 -38 64 43 -95 86 -88 -86 -119 5 -106 -14 109 34 116 -41 -77 -126 -11 50 -62 -87 -69 -119 -23 -93 -42 -95 105 55 -99 -91 74 51 -117
68 -27 -53 10 -52 -28 -112 -103 15 -60 22 2 71 -69 -41 -92 20 68 3 -57 -25 -28 22 120 -40 81 -6 91 108 -48 5 -90 47 -65 44 -114 -57 -114 52 73 85 108 119 67 123
57 -80 -32 -125 -16 -90 90 -35 0 -8 -34 -63 53 -106 123 88 9 14 57 109 -116 61 -82 97 87 -46 -96 30 34 -113 -117 -52 59 54 -2 -46 102 -27 109 89 -57 -62 -76 -86
62 -45 -42 125 123 -12 14 5 37 36 -106 109 84 -79 22 52 -114
```

14.113 seconds

Figure-4:EncryptedMessage

Once decryption occurs an original plain message is viewed by the client as in Figure-5. Because of using the dynamic key the encryption time and decryption time will be high if the key is lengthier. This becomes a drawback in this system.



SSL : DRSADS [Dynamic Rivest Shamir Adleman Digital Signature]

SSL:DRSADS[Dynamic Rivest Shamir Aldaman Digital Signature

5.16 seconds

Figure-5: Decrypted Message

7. CONCLUSION

The framework and development of SSL based load balancing on the essential secured generation technique in clustered web servers such as request and response are discussed. This approach has various advantages and disadvantages. According to the suggested SSL based load balancing algorithm proves the better performance. This work calculates parameters like Latency, Throughput, Coverage, and Security for measuring the performance. Then different load balancing algorithms are compared with various settings showed variation in latency. The developed model performance is compared with the previous study with benchmark existing SSL techniques suggested algorithm SSL based load balancing is also efficient in Secure Dynamic Web Server efficient load balancing.

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] Alla H.B., Alla, S.B., Ezzati, A. and Mouhsen, A., 2016, “A novel architecture with dynamic queues based on fuzzy logic and particle swarm optimization

algorithm for task scheduling in cloud computing". In International Symposium on Ubiquitous Networking Springer, Singapore. pp. 205-217.

[3] Alhassan Mohammed & Adjei-Quaye, Alexander, 2017, "Information Security in an Organization", International Journal of Computer (IJC), pp 100-116.

[4] Alkhudhayr .F, S. Alfarraj, B. Aljameeli and S. Elkhdiri, 2019, "Information Security:A Review of Information Security Issues and Techniques," International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-6.

[5] Amit Gajbhiye, Dr. Shailendra Singh, 2017, "Global Server Load Balancing with Networked Load Balancers for Geographically Distributed Cloud Data-Centres", International Journal of Computer Science and Network, pp. 682-688.

[6] Androutsellis-Theotokis S. and Spinellis, D., 2004. A survey of peer-to-peer content distribution technologies. ACM computing surveys (CSUR), 36(4), pp.335-371.

[7] Anitha T.N, Dr.R.Balakrishna, 2011, "An Efficient and Scalable Content Based Dynamic Load Balancing Using Multiparameters on Load Aware Distributed Multi-Cluster Servers", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 8, pp.6401-6411.

[8] Antonio Mana, Hristo Koshutanski, Ernesto J. Pérez, 2012, "A trust negotiation based security framework for service provisioning in load-balancing clusters", Computers & Security,Volume 31, Issue 1, pp. 4-25.

[9] Anurag M., Dharmendr S., 2011, "An Improved Backfilling Algorithm: SJF-BF", International Journal on Recent Trends in Engineering & Technology;3 /10/2011, Vol. 5 Issue 2, pp.78.

[10] Arti Mishra , 2015, "Network Load Balancing and Its Performance Measures",International Journal of Computer Science Trends and Technology (IJCST), Volume 3 Issue 1, pp.77-81.

[11] Blej M. and Azizi, M., 2016. "Comparison of Mamdani-type and Sugeno-type fuzzy inference systems for fuzzy real time scheduling". International Journal of Applied Engineering Research, 11(22), pp.11071-11075.

[12] Bora A. and Bezboruah, T., 2020. "Some Aspects of Reliability Estimation of Loosely Coupled Web Services in Clustered Load Balancing Web Server". In Critical Approaches to Information Retrieval Research, IGI Global, pp. 198-209.

[13] Butt M. A., & Akram, M. (2016). "A new intuitionistic fuzzy rule-based decision-making system for an operating system process scheduler", Springer Plus, pp. 1-17.